MYFLORIDANET-3

ITN NO: DMS-26/27-025

REVISED ATTACHMENT A

STATEMENT OF WORK AND CONTRACT DELIVERABLES

Table of Contents

SECTION 1.0 INTRODUCTION AND DEFINITIONS 12

1.1 INTRODUCTION 12

1.2 DEFINITIONS AND ABBREVIATIONS 12

SECTION 2.0 SCOPE OF WORK (TECHNICAL SOLUTION) 18

2.1 STAFFING PLANS (REPLY TAB 6) 18

2.1.1 Overall Staffing Plan 18

2.1.2 Staffing - Local Service Availability 18

2.1.3 Contractor Staffing Responsibilities 19

2.1.4 Ensuring Sufficient and Qualified Staff 20

2.1.5 Support Staffing 24

2.2 QUALIFICATIONS FOR PRIME RESPONDENT AND SUBCONTRACTORS 24

2.2.1 Business Proposal 24

2.2.2 Ability to Perform – Business Focus 25

2.2.3 Ability to Perform – Technical Focus 25

2.2.4 Dispute History 25

2.2.5 Experience for Enterprise Service Contracts (Reply Tab 4) 26

2.2.6 Business Qualifications 26

2.3 GENERAL REQUIREMENTS 26

2.3.1 Use of Manufacturer's Descriptive Text 26

2.3.2 Subcontracting Requirements 26

2.3.3 Flexibility to Quickly Modify Services 27
2.3.4 Service Testing Requirements 27
2.3.5 Operational and Contractual Oversight Role 27
2.3.6 Training on MFN-3 Technologies, Tools, and Services 28
2.3.7 Administrative Support and Technical Refresh 28
2.3.8 Support for Team Collaboration Tool 29
2.3.9 Inspection Process 29
2.3.10 Logging by Default 29
2.3.11 Operational Meetings 29
2.3.12 Surcharges and Fees 30
2.3.13 Naming Conventions 30
2.3.14 Network Time Service 30
2.3.15 Continuity of Operations Plan 30
2.3.16 Growth Planning 31
2.3.17 Multi-Factor Authentication 31
2.3.18 Vendor Access to Sites 31
2.3.19 SUNCOM Service Integration 31
2.4 WIDE AREA NETWORK ENTERPRISE SECURITY SERVICES 32
2.4.1 Enterprise Firewall 32
2.4.2 General Description - Operational Aspects of the Wide Area Network Enterprise Security Service 34
2.4.3 Security Operations Center (SOC) 35
2.4.4 Enterprise Security Information Event Manager Tool 36
2.4.5 Authentication Service 37

2.4.6 Assisting DMS in its Efforts Related to Security Compliance Audits, Training, and Awareness 37

2.4.7 Operational and Security Review of Logs and Interpretation of Traffic Flows 38

2.4.8 Security Logging Functionality and Review Strategies 38

2.4.9 Proactive and Reactive Security 38

2.4.10 Denial of Service and Distributed Denial of Service Protection 40

2.4.11 Attack Types 41

2.4.12 Individual IP Address Granularity and Maintaining Those Addresses 41

2.4.13 Denial of Service Customer Profile 41

2.4.14 Real-time Access to a Robust Reporting Dashboard (Customer Portal) .. 41

2.5 UNIVERSAL SERVICE FUND 42

2.5.1 Universal Service Fund Introduction 42

2.5.2 Maintaining Florida's E-rate Eligibility under MyFloridaNet-3 45

2.5.3 Services Provider's Liability for Maintaining Eligibility as a USF Service Provider 45

2.5.4 Eligibility under the USF E-rate program 45

2.5.5 E-rate Experience 46

2.5.6 E-rate Customer Care 46

2.5.7 E-rate Billing 46

2.6 BUSINESS OPERATIONS-REQUIREMENTS 47

2.6.1 General Description of the SUNCOM Business Model using Customer CSAB 47

2.6.2 Responsibilities of DMS and the Vendor in the SUNCOM Business Model 48

2.6.3 CSAB Interfaces with Vendors 49

2.6.4 Function Types in CSAB 50
2.6.5 Access Ordering Process 55
2.6.6 Mandatory interface with CSAB 56
2.6.7 Mandatory CSAB order 56
2.7 CORE FUNCTIONALITY AND RELATED SERVICES 56
2.7.1 General Core Services Infrastructure Requirements 56
2.7.2 MFN-3 Core Services Infrastructure Build-out Plan 57
2.7.3 Description of Proposed Virtual Routing and Forwarding (VRF) Structure(s) 58
2.7.4 Management Strategy and Structure 59
2.7.5 Core Internet 59
2.7.6 Enterprise Quality of Service (QoS) 60
2.7.7 MPLS 60
2.7.8 Multicast Functionality 60
2.7.9 MFN-3 Services Infrastructure Build-Out Plan Narrative 60
2.7.10 Highly Available and Highly Reliable Design Characteristics 61
2.7.11 High Availability and High Reliability Strategy for the MFN-3 Core Infrastructure Services 61
2.7.12 Physical Security as a component of High Availability and High Reliability 61
2.7.13 Power Supply as a component of High Availability and High Reliability 62
2.7.14 Minimal Convergence Times as a component of High Availability and High Reliability 62
2.8 ACCESS SERVICE – STATEWIDE WIDE AREA NETWORK (WAN) 62
2.8.1 High Availability and High Reliability Strategy for Access and Aggregation Services 62

2.8.2 Statewide Wide Area Network (WAN) Pricing 63
2.8.3 Multiple Paths Support into Core 63
2.8.4 End-To-End Integration 63
2.8.5 WAN - Underlying Technology and Interconnections with Partner Infrastructures 64
2.9 Metropolitan Area Network (MAN) Service 64
2.10 Point to Point Transport Services 65
2.11 Offnet Service - Cable Internet 65
2.12 Offnet Service - Cellular Internet 65
2.13 Offnet Service - LEO (Low Earth Orbit) Satellite Internet 66
2.14 Offnet Service - DIA (Dedicated Internet Access) 66
2.15 Other available Off-Net Transport Services 66
2.16 Daily Operational Management, Tools, and NOC 66
2.16.1 Day-to-day Responsibility is provided by the Services provider 66
2.16.2 Scope of Operational Management (Operational Support) 67
2.16.3 Network Operations Center 67
2.16.4 Services provider's Network Operations Center Implementation and Functionality 68
2.16.5 DMS Network Operations Center Oversight Responsibilities 68
2.16.6 Maintenance Notifications and Change Control Processes 69
2.16.7 Proposed Escalation Process 69
2.16.8 Effective Operational Management within Logical Partitions 70
2.16.9 Network Management System (NMS) and Security Tools Access 70
2.16.10 Internet Access to Tools 70
2.16.11 Customer Segregated NMS Views 70

2.16.12 Sharing Management Tools 70
2.16.13 Special Handling for Public Safety 71
2.16.14 Ticket Classifications Based on Problem Severity 71
2.16.15 Ticketing System Requirements 73
2.16.16 Proposed Ticketing System 74
2.16.17 Proposed Logging and Archival Process 74
2.16.18 Proposed Traffic Analyzer 75
2.16.19 Proposed SLA Performance Monitoring Service Functionality 75
2.16.20 Proposed Configuration Management System 76
2.16.21 Proposed Command Line Interface (CLI), SNMP and other Access Methods 76
2.16.22 Proposed Network Management System (NMS) 77
2.16.23 Proposed Performance Tools 77
2.16.24 Current Tools 78
2.17 CUSTOMER PREMISES EQUIPMENT – GENERAL 78
2.17.1 Acquisition and Support Specifications for Customer Premises Equipment Supported Under MFN-3 79
2.17.2 Authentication, Authorization, and Accounting (AAA) 79
2.17.3 Certified Customer Premises Equipment (CPE) List 80
2.17.4 Certified CPE List Process 80
2.17.5 Bi-directional Forwarding Detection (BFD) 81
2.17.6 Operational Parameters Related to Customer-Managed CPE Configuration 81
2.17.7 Services Provider-Managed Configuration Management 81

2.17.8 Virtual Routing and Forwarding (VRF)-Enabled CPE and VRF-Lite Configuration Support 82
2.17.9 Customer Premises Equipment Response Requirements 82
2.17.10 Customer Premises Equipment Rental Option and Price Protection 82
2.17.11 Return and Removal of CPE: 83
2.18 REMOTE ACCESS -- CENTRALIZED VIRTUAL PRIVATE NETWORK 83
2.18.1 Centralized VPN Service for MFN-3 Remote Access 83
2.18.2 Remote Site to Centralized VPN Gateway (LAN-to-LAN VPN) 84
2.18.3 Redundancy for the Centralized VPN System Components 85
2.18.4 Remote User Access Control Mechanisms 86
2.18.5 Network Address Translation (NAT) 86
2.18.6 Installation, Monitoring, and Trouble Reporting for LAN-to-LAN VPN 86
2.18.7 IKE, IPSec Security Association (SA) and SSL Attribute Matrix 87
2.18.8 Client to LAN Remote User to Centralized VPN Gateway (Client-to-LAN VPN) 88
2.18.9 Client-to-LAN VPN Split-Tunneling and Security Policy Compliance 88
2.18.10 Multi-Factor Authentication Requirement 89
2.18.11 Username/Password Policy Enforcement 89
2.18.12 Inactivity and Duration Timeouts for Client to LAN Sessions 90
2.18.13 In Case of Emergency (ICE) VPN Accounts 90
2.18.14 Test VPNs for DMS 90
2.18.15 End-to-end Integration Responsibility 90
2.18.16 VPN Customer Migration 91
2.19 VPN TO MFN-3 91
2.19.1 VPN to MFN-3 Monitoring and Operational Management 92

2.20 SD-WAN Software Defined Wide Area Network 92
2.20.1 Installation, Monitoring, and Trouble Reporting for SD-WAN 94
2.20.2 Contractor Provided SD-WAN CPE Appliance 94
2.21 SASE Secure Access Service Edge 95
2.22 Cloud Transport 96
2.23 Ancillary Network Services – General 97
2.23.1 Telecommunication Service Priority 97
2.23.2 Demarcation Extension Service 97
2.23.3 After-Hour Installation Services 98
2.23.4 Expedited Installation Services 98
2.24 Miscellaneous Conditions 98
2.24.1 No Cost Increase 98
2.24.2 Third Party and/or Independent Charges 98
2.24.3 Florida Administrative Code 98
2.24.4 No One-Time or Non-Recurring Charges 99
2.24.5 Proposed Equipment (CPE and MFN-3 Services Infrastructure) 99
2.24.6 Services provider Responsibility for Infrastructure Upgrades 99
2.24.7 Engineering Support 99
2.24.8 CPE Configuration Templates for Customer Managed CPE 100
2.24.9 Operational Change Request Process 100
2.24.10 Authentication Server and Logs 100
2.24.11 Using Standards and Templates 100
2.24.12 Customer Responsibilities for On-Site Contact Information 100
2.24.13 Single Point of Contact 101

2.24.14 Non-Contiguous IP Address Blocks 101
2.24.15 Urgent Bandwidth Increase 101
2.24.16 Network Management System updates 101
2.24.17 Turn-Up Support for Customer-Provided CPE 101
2.24.18 SUNCOM or MFN-3 Brand 101
2.24.19 MFN-3 Marketing Initiatives 101
2.24.20 Acceptance Criteria 101
2.24.21 Criteria for IMAC Signoff and Billing Start 102
2.24.22 Bill Stop Date 102
2.24.23 Invoices 102
2.24.24 Guaranteed Bandwidth Speed 102
2.24.25 Month-to-Month Term 102
2.24.26 Operational Guide 102
2.24.27 Quantity or Revenue Guarantees 102
2.24.28 Published Rates Include the DMS Administrative Fee 103
2.24.29 Statewide Uniformity 103
2.24.30 Standard Operating Procedures 103
2.24.31 No Upfront Costs to DMS for the Implementation of the MFN-3 Infrastructure 103
2.24.32 Travel 103
2.24.33 Labor 103
2.24.34 Enable Features, Functionality and Configuration Changes 103
2.24.35 Connections/Links Utilization 103
2.24.36 NMS and Security Tools Metric Alerts 104

2.24.37 Delivery of All Services 104
2.24.38 Final Determination 104
2.25 PROJECT MANAGEMENT 104
2.25.1 Project Charter and Project Management Plan 105
2.25.2 Project Management Implementation Phase 106
2.25.3 Project Management - Guides 107
2.25.4 Project Management - Closure 108
2.25.5 Project Management Implementation and Migration Plans 108
SECTION 3.0 PERFORMANCE MEASURES (SERVICE LEVEL AGREEMENTS - SLAS) 109
3.1 PERFORMANCE MEASURES 109
3.1.1 SLA Criteria 109
3.1.2 Service Credits 112
3.1.3 Performance Monitoring Baseline 112
3.1.4 Scrubbing Alerts 112
3.1.5 Dynamic SLAs 113
3.1.6 Timely Credit Determination and the Application of Credits 113
3.1.7 Scrubbing Alerts Production Implementation 113
SECTION 4.0 FINANCIAL CONSEQUENCES FOR NON-PERFORMANCE 113
4.1 WITHHOLDING PAYMENT OR OTHER REMEDIES 113
4.1.1 Consequences for Non-Performance 113
SECTION 5.0 SLA MIGRATION AND TRANSITION PLANNING (SUPPORT SERVICES) 114
5.1 MIGRATION FROM MFN-2 TO MFN-3 114
5.1.1 MFN-3 Core Services Readiness Plan 114
5.1.2 Migration Plan – Sites and Services 115
5.1.3 Migration - Staffing Resource Requirements 115

5.1.4 Migration - Knowledge Transfer 116
5.1.5 Migration – Project Management Tasks and Related Deliverables 116
5.1.6 Migration - Communication Plan 116
5.1.7 Migration - Engineering Review 117
5.1.8 Migration - Provisioning Planning 117
5.1.9 Migration - Network Operations Center 118
5.1.10 Migration - Administrative Services 118
5.1.11 Migration - Payment Strategy Connection-By-Connection 118
5.1.12 Migration - Connection Testing Period with Fall Back Option 118
5.1.13 Migration - Special Construction 119
5.2 TRANSITION BETWEEN MFN-3 AND THE SUCCESSOR CONTRACT 119
5.2.1 Transition Introduction 119
5.2.2 Transition - Contract Completion 119
5.2.3 Transition - Payment Strategy Connection-By-Connection 119
5.2.4 Transition - Overlapping Contracts 119
5.2.5 Transition - Contract Terms, Conditions, and Rates 119
5.2.6 Transition - New Work Orders during Transition Period 120
5.2.7 Transition - Expeditious Efforts during the Transition 120
5.2.8 Transition - End of Contract Transition Assistance 120

SECTION 1.0 Introduction and Definitions

1.1 Introduction

This Attachment A contains the Statement of Work (SOW) under any resulting Contract from this ITN for MFN-3 Services, including core and last mile. The SOW includes the Scope of Work, Performance Measures, Financial Consequences for Non-Performance, and Migration and Transition Plan requirements.

The overall deliverable to be received by MFN-3 Customers is a highly available, highly reliable, robust network that will support voice, video, and data. The specific deliverables are established throughout this SOW. Service Level Agreements (SLAs), in Statement of Work Section 3 and **Attachment C, Service Level Agreements**, define the required minimum level of service to be performed which includes criteria for evaluating successful service. The Services Provider shall satisfy all of the criteria the earlier of a. the dates defined in the SLAs, b. the expiration date of the Contract, or c. the expiration dates of any purchase orders for the Contract.

DMS requires an Enterprise solution provided by a single Services provider managing existing telco partnerships for local loop, where required.

This SOW is intended to reflect the requested service components DMS is seeking the Respondent to offer MFN-3 Services. The SOW includes references to service components that "must", "shall", or "will" be delivered; however, these SOW references to "must", "shall", "will" and "minimum requirements" will not affect DMS's determination of a Respondent's responsiveness. DMS intends for these SOW references to become mandatory at the time of Contract execution (as reflected in DMS's Request for Best and Final Offer). However, these SOW references may be subject to negotiation during the procurement and will be resolved through the terms of DMS's Request for Best and Final Offer. The Request for Best and Final Offer may also identify contractual requirements in place of previous requests for responses. For example, the word 'should' may be replaced by the word 'must' in the final SOW attached to the Request for Best and Final Offer.

1.2 Definitions and Abbreviations

1. **Billed Entity Applicant Reimbursement (BEAR):** Applicants file an FCC Form 472 (BEAR Form) to request reimbursement from USAC for the discounted cost of eligible equipment and services approved on the FCC Form 471, and which the applicant has received and paid in full to its service provider.
2. **Bi-directional Forwarding Detection (BFD):** A media and protocol independent liveliness detection mechanism used to detect link failures in situations where the existing failure detection methods are either not present, or do not offer fast enough convergence times
3. **Command Line Interface (CLI):** A mechanism for interacting with a computer operating system or software by typing commands to perform specific tasks; instructing a system to perform a given task "entering" a command. After the user submits the text command and presses the "Enter" key the command-line interpreter receives, analyzes, and executes the requested command.

4. **Client:** Computer hardware or software that accesses a service made available by a server. For example, web browsers are clients that connect to web servers.
5. **Contract:** The legally enforceable agreement that results from the underlying solicitation (ITN No.: DMS-26/27-025). The parties to the Contract will be the Department and Contractor.
6. **Contractor:** The Respondent that will be awarded a Contract pursuant to the underlying solicitation (ITN No.: DMS-26/27-025). In this contract, the Contractor is typically referred to as the Services Provider.
7. **Continuity of Operations Plan (COOP):** A plan to ensure that mission-essential functions continue in the event personnel and/or facilities are adversely impacted by a disaster in conjunction with the DMS COOP required by s. 252.365, F.S. Authorization form used by DMS's eligible user community to order services under the Contract.
8. **Core Services Infrastructure:** Refers to the portion of the network provided by the Services Provider to facilitate interconnectivity between State agencies and other agency users, as well as the overall Internet for connections traversing the MFN-3 Core Network. This is inclusive of all components in the IAGs and POPs.
9. **Communications Service Authorization and Billing (CSAB) System:** A centralized web application used for SUNCOM services.
10. **Customer:** The State agency or other entity identified as the party to receive commodities or contractual services from the Contractor under the Contract resulting from the underlying solicitation (ITN No.: DMS-26/27-025). Customer may be used interchangeably with SUNCOM Customer and MFN-3 Customer.
11. **Datagram Transport Layer Security (DTLS):** A security protocol based on Transport Layer Security (TLS), it brings strong encryption and privacy to connectionless protocols like UDP, preventing eavesdropping and tampering in real-time applications without adding connection delays
12. **Department:** The Department of Management Services as defined by section 20.22, Florida Statutes (F.S.). Also referred to herein as "DMS."
13. **Demilitarized Zone (DMZ):** A physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has direct access to equipment in the DMZ, rather than any other part of the network.
14. **Domain Name System (DNS):** Hierarchical naming system that associates various types of information with domain names translating them into numerical (binary) identifiers, mapping fully qualified domain names to IP addresses and vice versa.
15. **Denial-of-Services (DoS) Attack:** Any efforts of a person or a group to prevent a public or private site service from functioning efficiently or not at all, temporarily or indefinitely.
16. **Enhanced 911 (E911):** System that automatically associates a physical address with the 911 caller's telephone number and routes the call to the most appropriate Public Safety Answering Point (PSAP) for that address and

provides both the caller's location and calling party's telephone number for emergency services.

17. **Expedited Forwarding (EF):** Type of class or Differentiated Services Code Point (DSCP) value assigned in networks to prioritize voice traffic.
18. **End-of-Life**: A formal manufacturer designation marking the phase-out of a specific hardware or software product.
19. **End-of-Support (EOS):** The date on which any hardware, software, or other product (i) is no longer supported, maintained, updated, or patched by its manufacturer; (ii) no longer receives security updates bug fixes, or technical support; or (iii) in DMS' reasonable judgment, can no longer be maintained in compliance with the performance, security, or service level requirements of the Contract. EOS is not dependent upon or limited to any formal "end of support," "end of life," or similar designation by the manufacturer or publisher**.**
    Enterprise: A large-scale, interconnected network with physical, virtual, and logical communication infrastructure that supports the daily operations of an organization.
20. **Ethernet Virtual Circuit (EVC):** A logical, Layer 2 service connection that associates two or more Customer endpoints across a service provider's network.
21. **E-rate:** The Schools and Libraries Program of the Federal Universal Service Fund (USF). The program provides discounts to assist eligible K-12 schools and libraries in obtaining eligible telecommunication services, telecommunications, Internet access, internal connections, and internal connections maintenance as defined in the annually published Eligible Services List.
22. **Florida Information Resource Network (FIRN):** A data network for public schools, colleges, universities and libraries.
23. **High availability and high reliability (HA/HR):** Describes a system being available and producing the correct results over time.
24. **Individual Case Basis (ICB):** Describes situations where DMS will make a determination on issues that require a resolution based on the unique circumstances of the issue.
25. **Internet Engineering Task Force (IETF):** The IETF is a large, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
26. **Internet Access Gateway (IAG):** A hardware or software network device or point that acts as the interface or bridge between a private network (Like MFN-3) and the Internet, allowing devices on the private network to access the broader Internet and vice versa. The device manages the flow of packets between the two and can also provide services such as routing and firewall filtering.
27. **Internet**: The Internet is referencing the global collection of interconnected networks used to facilitate communications and commerce around the world.
28. **Invitation to Negotiate (ITN)**: This competitive solicitation. Also referred to herein as "ITN" or "solicitation."
29. **Internet Protocol Flow Information Export (IPFIX):** An IETF protocol, used to provide a standard for exporting for Internet Protocol flow information from

routers, probes and other devices that are used by mediation systems, accounting/billing systems and network management systems to facilitate services such as measurement, accounting and billing.

30. **Jitter:** The time variation of a periodic signal often used as a measure of the variability over time of the packet latency across a network. It is abrupt and unwanted variations of one or more signal characteristics, such as the interval between successive pulses, the amplitude of successive cycles, or the frequency or phase of successive cycles.
31. **Latency:** The amount of time delay between the initiation of a service request for data transmission, or when data is initially received for retransmission, to the time when the data transmission service request is granted, or when the retransmission of data begins. Latency is measured either one-way (the time from the source sending a packet to the destination receiving it), or round-trip (the one-way latency from source to destination plus the one-way latency from the destination back to the source).
32. **Local Area Network (LAN):** A computer network covering a small geographic area, like a home, office, or small group of buildings, such as a school, or an airport; LANs have higher data-transfer rates due to smaller geographic area.
33. **Local Loop**: Final leg of the telecommunications network that delivers services to end-user's facilities. It's the portion of the network that connects the service provider's infrastructure (like a central office, wire center or local exchange) to the Customer premises.
34. **Low Earth Orbit (LEO) Satellite:** Equipment that orbit the Earth at lower altitudes than standard satellites, facilitating high-speed network connectivity. LEO satellites are often operated as a cluster to provide connectivity to a broad geographical area.
35. **Metropolitan Area Network (MAN):** A large data network that usually spans a city or a large campus. A MAN usually interconnects a number of local area networks using a high-capacity backbone technology, such as fiber-optic links, and provides up-link services to wide area networks and the Internet.
36. **Multi-factor authentication (MFA):** An authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or VPN.
37. **MyFloridaNet-2** (**MFN-2):** The current telecommunications network used by Florida's agencies and other eligible users. The statewide infrastructure is designed to be a highly available, highly reliable, robust core able to support inter-site connections and access the Internet.
38. **MyFloridaNet-3 (MFN-3):** The follow-on telecommunications network which will replace MyFloridaNet-2.
39. **MFN-3 Services Infrastructure:** A specific term used to indicate the entirety of the statewide communications infrastructure. These components include but are not limited to core backbone facilities, core and aggregate equipment, Internet Gateway equipment, enterprise firewalls, DDoS mitigation systems, staffing, NOC, NMS and security tools, SOC, SD-WAN and Centralized VPN, and licenses.
40. **Multi-Protocol Label Switching (MPLS):** Directs and carries data from one network node to the next; a data-carrying mechanism where data packets are assigned labels. Packet-forwarding decisions are made solely on the contents

of this label, without the need to examine the packet itself allowing the creation of end-to-end circuits across any type of transport medium, using any protocol.

41. **Mean-time-to-repair (MTTR):** Basic measure of the maintainability of repairable items; the total corrective maintenance time divided by the total number of corrective maintenance actions during a given period of time.
42. **Network Addressing Translation (NAT):** The process of modifying network address information in datagram packet headers while in transit across a traffic routing device, for the purpose of remapping a given address space into another; involves re-writing the source and/or destination IP addresses and usually the TCP/UDP (User Datagram Protocol) port numbers of IP packets as they pass through.
43. **Network Management System (NMS):** A combination of hardware and software used to monitor and administer a network.
44. **Network-to Network Interface (NNI):** The boundary or point of interaction between network service providers that serves as the technical boundary where protocol issues are resolved and as the point of division between the responsibilities of the individual service providers.
45. **Network Operations Center (NOC):** A collection of staff and support tools used to monitor and coordinate activities. Under this Statement of Work, the NOC provides 24x7x365 monitoring support for Florida's statewide communications network, MyFloridaNet.
46. **Original Equipment Manufacturer (OEM)**: A company that produces components or products sold to other companies to be integrated into their products.
47. **Point of Presence (POP):** One of several locations at which the MFN-3 Core node infrastructure connects to the Internet. Refers to the location as well as the hardware necessary to facilitate the connection.
48. **Public Safety Answering Point (PSAP):** The public safety agency that receives incoming 911 requests for assistance and dispatches appropriate public safety agencies to respond to the requests in accordance with the State E911 plan.
49. **Quality of Service (QoS):** Resource reservation control mechanisms with the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.
50. **Remote Partner:** External entity connected via VPN to MFN-3.
51. **Reply:** The formal response to an ITN.
52. **Respondent:** A Services Provider who submits a Reply to this ITN.
53. **Read-only (RO):** Grants the ability to view/access "show commands" without permission to modify.
54. **Read/Write (RW):** Grants the ability to change system parameters.
55. **Role Based Access Control (RBAC):** A security method that restricts system access based on user roles.
56. **Secure Access Service Edge (SASE)**: A cloud architecture model that combines network and security-as-a-service functions together and delivers them as a single cloud service. Conceptually, SASE extends networking and security capabilities beyond where they're typically available.

57. **Software-Defined Wide Area Network (SD-WAN)**: A virtual WAN architecture that allows the leveraging of any combination of transport services including MPLS, LTE and DIA services to securely connect users to applications.
58. **Services Provider:** The Contractor selected to provide Services, pursuant to this solicitation. The Services Provider will be the ITN Respondent that is awarded the services described in this Contract.
59. **Security Information and Event Management (SIEM):** A software solution that collects security data from an organization's network, servers, and apps, centralizes it, and analyzes it in real time to help teams detect, investigate, and stop cyber threats
60. **Site Inventory:** The list of locations with services installed under MyFloridaNet, and FIRN. The Site Inventory provides details such as the physical location, access technology, and bandwidth.
61. **Service Level Agreement (SLA):** A part of the formal, legally binding contract between a service provider and ~~a Customer~~ the Department that defines the expected quality, performance and responsibilities of both parties
62. **Simple Network Management Protocol (SNMP):** A UDP-based network protocol used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.
63. **Security Operations Center (SOC):** A centralized support unit on an organizational and technical level in the Contractor's organization to deal only with security issues.
64. **Service Provider Invoice (SPI):** Service providers file an FCC Form 474, (Service Provider Invoice (SPI) Form) to request reimbursement from USAC for the discounted portion of costs for eligible equipment and services provided to the applicant and approved on the FCC Form 471 and provided to the applicant. The Services Provider must provide the equipment and services and bill the applicant for their non-discounted share before submitting a SPI Form to USAC. The applicant is obligated to pay their share.
65. **Secure Shell (SSH):** A network protocol that allows data to be exchanged using a secure channel between two networked devices; typically used to log into a remote machine and execute commands.
66. **State:** The State of Florida.
67. **Transport Layer Security (TLS):** A protocol that provides encryption, integrity, and authentication. It is the modern update to the older SSL (Secure Sockets Layer) protocol.
68. **Type I Circuit:** Circuit that is delivered where the entire EVC path stays within a single carrier's infrastructure.
69. **Type II Circuit:** Circuit that is delivered where the entire EVC path traverses two carriers' infrastructure.
70. **USAC:** Universal Service Administrative Company – Entity responsible for administering the Universal Service Fund under the direction of the Federal Communications Commission.
71. **Unique Service Identifier** (**USI):** Used as an intelligent name for NOC monitoring.
72. **Vendor:** An entity that is capable and in the business of providing a commodity or contractual service similar to those within this solicitation.

73. **Virtual Local Area Network (VLAN):** A computer network using inter-networks as data links that are transparent for users and do not have restrictions on protocols, so that the network has the characteristics/attributes of a physical local area network but allows end stations to be grouped together even if they are not located on the same network switch.
74. **VPN:** Virtual Private Network. A computer network implemented in an additional software layer (overlay) on top of an existing larger network for the purpose of creating a private scope of computer communications or a secure extension of a private network into an insecure network such as the Internet.
75. **Virtual Routing and Forwarding (VRF):** A technology that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other.
76. **Virtual Tunnel Interface (VTI):** A logical, route-based interface used to establish secure IPSec VPN connections
77. **Wide Area Network (WAN):** A data network that covers a broad area; used to connect Local Area Networks (LANs) and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations (i.e., any network whose communications links cross metropolitan, regional, state or national boundaries).
78. **Wire Center**: A physical facility that serves as a hub for distributing telephone and data services within a specific geographic area. A physical location within an LEC's central office or other provider's facility where local loops (the wires that connect to Customer premises) are terminated.

SECTION 2.0 SCOPE OF WORK (TECHNICAL SOLUTION)

2.1 Staffing Plans (Reply Tab 6)

In addition to staff positions listed under these subsections, the Contractor shall provide sufficient, qualified personnel to oversee and carry out the services of this Contract.

The term “Contractor staff” includes all staff employed by the Contractor and by its subcontractors relevant to the Contract.

Unless otherwise specified, the Services Provider staff may not be subcontracted without written DMS approval.

2.1.1 Overall Staffing Plan

Project Staffing Plan Description and Worksheets: Provide a narrative description of the proposed Staffing Plan in-line below. The narrative response should describe how the proposed staffing plan will meet the needs for MFN-3. In addition to the narrative description, also complete **Attachment H, Staffing Plan Worksheet**, for key staff positions, including after-hours contacts. Resumes are not requested.

2.1.2 Staffing - Local Service Availability

At the discretion of DMS, contractors are required to make resources physically available in Tallahassee within 48 hours to provide timely responses to service needs.

Include in the **Attachment H, Staffing Plan Worksheet**, the roles and responsibilities of the proposed team members and their availability to meet in Tallahassee as needed. Describe how these staff will interface with DMS to address technical and administrative support issues.

2.1.3 Contractor Staffing Responsibilities

The Contractor staff responsibilities include conducting all components of the Contract in a timely, efficient, productive, consistent, courteous and professional manner as representatives of the State.

The Contractor staff shall devote the time and resources necessary to successfully manage the State of Florida account, including being available for telephonic, email and on-site consultations.

The Contractor shall provide each Contractor staff member orientation and training on all components of the Contract prior to working on any component of the Contract. Documentation of this training shall be provided to DMS upon request.

The Contractor shall be required to employ the required key staff positions described in this SOW.

It is understood and agreed that from time to time a vacancy may occur in required key staff positions. For purposes of this Contract, a vacant position is defined to occur when the position is not initially filled, the employee assigned to the position has resigned, been terminated, reassigned, or is filled with a person who does not possess the minimum qualifications required to perform the job duties. A vacancy does not occur when an employee is temporarily absent due to vacation, sick leave, or other temporary leave condition such as training. In the case of a vacancy, the Contractor may arrange for the job duties to be provided by another employee who meets the minimum job qualifications until this position is filled. However, a temporary assignment will not put the SLA clock on hold.

The Contractor agrees to fill all required key staff positions within thirty (30) days from Contract execution and within ninety (90) days after the date upon which the position becomes vacant. The Contractor may request a waiver from DMS if it believes it has good cause to not fill a required key staff position within the ninety (90) days allowance. Contractor will submit waiver requests to the DMS Contract Manager. DMS will review the requests on a case-by-case basis and respond within a reasonable timeframe. DMS reserves the right for final determination on all waiver requests. Positions not filled within the ninety (90) day timeframe, or otherwise waived by DMS, will incur an SLA violation.

The Contractor shall notify DMS of any vacancy of a required key staff position within two (2) business days of the vacancy occurring.

The Contractor will only fill required key staff positions with persons that fulfill the minimum job qualifications set forth in this SOW Section 2.

DMS reserves the right to review and approve candidates being considered by the Contractor for employment for a required key staff position described in this Contract.

DMS will have the right to request the replacement of any staff who serve in a required key staff position, any staff part of the Customer Support Team, or any staff part of the Network Operations Center (NOC) or Security Operations Center (SOC). Contractor will remove such staff within thirty (30) calendar days or earlier upon DMS' notice to Contractor.

The Contractor must provide sufficient Contractor Staff to handle the workload projected for the start of the Contract and shall be scalable and flexible, so it can be adapted as needed.

The Contractor must develop and maintain a final Staffing Organizational Chart that includes all staff resources that will be assigned to all components of the Contract to be approved by DMS no later than thirty (30) calendar days from Contract execution. The final Staffing Organizational Chart must contain names, titles, and number of staff (full-time and part-time) proposed to support the State of Florida. The Contractor's final Staffing Organizational Chart shall include a justification for the number of staff, the percentage of time each staff person will devote to the Contract.

In the event DMS determines the Contractor's staff or staffing levels are not sufficient to properly complete the services specified in this Contract, it shall notify the Contractor in writing. The Contractor will have ninety (90) calendar days to remedy the identified staffing deficiencies.

Given the statements in this subsection, describe in detail the proposed offering for this subsection. Provide a detailed description of the following:

- How Respondent will ensure the dedication of its proposed required key staff positions, including the proposed percent of time dedicated to DMS;
- How Respondent will utilize staffing resources beyond those required for day-to-day (standing) operational, Customer-facing, and management activities.

2.1.4 Ensuring Sufficient and Qualified Staff

2.1.4.1 Account Manager

Contractor shall assign a dedicated, but not necessarily exclusive, Account Manager as the primary contact for DMS, unless DMS determines an exclusive Account Manager is in DMS's best interest. This is a required key staff position.

The Contractor is required to provide an Account Manager for all contracted services. The Account Manager will be the senior manager and primary contact with responsibility for all MFN-3 issues, including, but not limited to, day-to-day coordination and resolution of all MFN-3 activities. The Account Manager will be a senior staff member able to carry DMS concerns to the Contractor's management personnel. The Account Manager or designated backup(s) must be available to DMS twenty-four hours a day, 365 days of the year.

The Account Manager will be required to participate in all workgroups created by the Contractor or DMS related to MFN-3.

The Account Manager shall possess the following minimum qualifications:

- Minimum five (5) years' experience working with government clients in a government account management or sales role.

- Knowledge of government business practices, which is inclusive of State of Florida practices and practices of authorized users.
- Minimum of five (5) years' work experience in the telecommunications industry.
- Strong verbal and written communication skills, including the ability to communicate effectively at all levels of the organization.

2.1.4.2 Project Manager

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

The Project Manager shall oversee and take on the responsibility for the success of all projects. Projects include, but are not limited to, Contract Implementation and Migration, agency specific Implementation and Migration, and Post Migration Steady State. This individual will be the single point of contact to the State coordinating all work and communications with DMS. This individual will manage and direct the planning of the Contractor's staff and resources.

The Project Manager will participate in various MFN-3 workgroups.

The Project Manager shall possess the following minimum qualifications:

- Ability to be responsible for all aspects of any projects related to this Contract.
- Ability to lead and direct teams to deliver projects within the constraints of schedule, budget and resources.
- Demonstrate sufficient knowledge and experience to appropriately apply a project management methodology to projects
- Experience using Microsoft Project and the ability to keep all projects updated frequently and accurately.
- Currently holds either Project Management Professional certification from the Project Management Institute, a Certified Scrum Master from Scrum Alliance, CompTIA Project+ certification from CompTIA, a Lean Six Sigma certification, or other equivalent project management certification approved in writing by DMS.

2.1.4.3 Business Operations Manager

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

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

The Business Operations Manager will participate in various MFN-3 workgroups.

The Business Operations Manager shall possess the following minimum qualifications:

- Minimum five (5) years' experience working with Government clients.
- Knowledge of government business practices, which is inclusive of State of Florida practices and practices of authorized users.
- Strong verbal and written communication skills, including the ability to communicate effectively at all levels of the organization.

2.1.4.4 Senior Engineering and Design Manager

Contractor shall assign a dedicated Senior Engineering and Design Manager. This is a required key staff position.

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

The Senior Engineering and Design Manager will participate in various MFN-3 workgroups.

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

- Minimum of five (5) years' experience leading an engineering team responsible for services similar in size and scope to MFN-3 services
- A master's degree or higher in an engineering discipline and five (5) years or more of documented relevant work experience. Equivalent foreign degrees are also acceptable. Ten (10) years' documented work experience in a relevant field can substitute the master's degree requirement.

2.1.4.5 Senior Operations and Security Managers

Contractor shall assign dedicated, but not necessarily exclusive, Operations and Security Managers unless the Department determines an exclusive Operations or Security Manager is in DMS's best interest. This is a required key staff position. The Operations and Security Managers are two distinct positions that will participate in the various workgroups to accomplish MFN-3 services.

The Operations and Security Managers shall serve as the engineer capable of communicating with other engineers as needed to resolve day-to-day issues. The individual will function as a single point of contact for the day-to-day networking, service, and security issues, typically those involving real-time concerns. The individuals must have the authority to direct the Contractor's staff. The Operations and Security Managers, or a designated backup(s), must be available twenty-four hours a day, 365 days of the year as required to manage the NOC and SOC concerns, and respond to State requests.

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

- A master's degree or higher in an engineering discipline and five (5) years or more of documented relevant work experience. Equivalent foreign degrees are also acceptable. Ten (10) years' documented work experience in a relevant field can substitute the master's degree requirement.
- Experience with business continuity and disaster recovery, including experience in development of disaster recovery plans.
- Experience with information security architecture and security tools.
- Knowledge of telecommunications industry best practices for service performance and security, and applicable laws and regulations as they relate to security.
- Knowledge of current technologies and processes used to establish and maintain networks with respect to security of MFN-3.

It's preferred but not required that the Senior Operations & Security Managers hold Certified Information Security Manager, Certified Information Systems Security Professional, or other industry recognized security certification.

2.1.4.6 Customer Support Team

The Contractor shall provide a Customer Support Team, which is not required to be full-time or dedicated to this Contract. This team is not considered a key staff position or positions. The Customer Support Team shall be sufficiently qualified and trained to provide the following:

- Timely Customer training by the Contractor's team in reaction to changes in services and features offered.
- Resolve service requests timely
- Full staffing for projects to implement new technologies, related services, and equipment features that are supported by the industry
- Timely closure for operational changes
- Meet all service delivery due dates

The Customer Support Team shall include at least one (1) named individual to act as the CSAB Administrator.

2.1.4.7 Network Operations Center & Security Operations Center Staffing

The Contractor shall provide dedicated NOC and SOC staffing. This staffing is not considered a key staff position or positions. The NOC and SOC staffing shall be sufficiently staffed, qualified and trained to provide the requirements as detailed in SOW including but not limited to the following:

- Staffing for the NOC and SOC twenty-four hours a day, 365 days of the year.
- Proactive NOC and SOC monitoring including issue resolution.
- Staffing for the NOC and SOC that are certified, experienced, well-trained, and well-equipped professionals.
- NOC and SOC staff access to Contractor's advanced research team that will assist in identifying threats and developing preventative counter measures based on information collected from monitoring events worldwide. The Contractor's advanced research team will consist of cyber threat researchers that are assigned to the pursuit of existing and emerging global cyber threats.

The advanced research team will research the global landscape, perform in-depth analysis of emerging threats, and develop counter measures to protect MFN-3 Customers.

Given the statements for staff positions in 2.1.4.1 through 2.1.4.7 provide the following:

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

Provide a proposed Staffing Organizational Chart, including titles and number of staff (full-time and part-time) proposed to support the State of Florida.

2.1.5 Support Staffing

In addition to the above staff, the Contractor will be required to provide sufficient and qualified staff to meet the needs of the MFN-3 Contract. At a minimum, propose detailed descriptions for the staff listed below. Describe Respondent's proposed staffing levels, minimum qualifications, and average years of experience of the team.

- Network Management System and Security Tools Support
- Programming Support for CSAB and Contractor's System
- Tier 1, 2, 3 Engineering Support
- Field Technicians
- Other

2.2 Qualifications for Prime Respondent and Subcontractors

The reply to this Section must be entered after each subsection below for both the Prime Respondent and all proposed subcontractors. Under each subsection below, provide a narrative response that addresses the criteria for both the Services Provider and for each proposed subcontractor[s].

The information to be entered after each subsection listed below will supplement basic information provided in **FORM 6 – BUSINESS QUALIFICATIONS & EXPERIENCE QUESTIONNAIRE** and information provided in **FORM 3 – SUBCONTRACTING.** As explained in Section 4.3 of the ITN, evaluators will receive completed copies of a Respondent's FORM 6 and FORM 3 along with responses provided to the questions below provided in a Respondent's Technical Reply.

2.2.1 Business Proposal

Provide the following:

- A description of how the Respondent's MFN-3 business proposal will provide the best value to the State.
- A description of the Respondent's understanding of MFN-3 needs, and the requirements of the State.
- A description of any letters of intent, memoranda of understanding, subcontracts, or other agreements between the Respondent and subcontractor[s] relating to the potential and scope of work to be performed under the Contract.
- For proposed subcontractors, provide the following:

- Information on the role, responsibilities, and duties, explaining the services to be performed by the subcontractor[s].
- The percentage of the total estimated contract value that will be performed by each subcontractor.

2.2.2 Ability to Perform – Business Focus

Provide the following:

- Supporting detail demonstrating the ability to provide the services described in this solicitation based upon past professional experience and performance.
- Details on the approach to Customer service in terms of service establishment, trouble reporting and tracking, work ordering, and billing in contracts similar to MFN-3.

This information is not a duplicate of the market position/penetration information provided above under business qualifications; this information is expected to have a business focus.

2.2.3 Ability to Perform – Technical Focus

Provide the following:

- Supporting detail demonstrating the ability to provide the services described in this solicitation based upon their past professional experience and performance.
- Details on the approach to Customer service in terms of establishing a network, technical standardization, technical support, and technical competence in contracts similar to MFN-3.

This information is not a duplicate of the market position/penetration information provided above under business qualifications; this information is expected to have a technical focus.

2.2.4 Dispute History

The term “contract disputes” means any circumstance involving the performance or non-performance of a contractual obligation that resulted in: (i) identification by the contract Customer that either the Respondent or any subcontractors were in default of a duty under the contract; (ii) the issuance of a notice of default or breach; (iii) the institution of any judicial or administrative action as a result of the alleged default or defect in performance; or (iv) the assessment of any fines or liquidated damages under such contracts.

- Identify all contract disputes (including Respondent, its affiliates, subcontractors, agents, etc.) with any government agency Customer within the last five years related to contracts where Enterprise networking services were provided.
- Indicate whether the disputes were resolved and, if so, explain how they were resolved.

2.2.5 Experience for Enterprise Service Contracts (Reply Tab 4)

Submit reference documentation as described below for similar contracts. In order to qualify as appropriate experience, services must be ongoing or must have been completed within the past ten (10) years preceding the issue date of this solicitation.

For each of the contract references use the Business/Corporate Reference, **FORM 6 - QUALIFICATIONS & EXPERIENCE QUESTIONAIRE** to provide contact information.

For each reference provided on **FORM 6 - QUALIFICATIONS & EXPERIENCE QUESTIONNAIRE**, provide in this subsection, the name of the Contract including the name of the organization(s) contracted with, and the following:

- Contact information enabling verbal confirmation of the Customer reference.
- A detailed description of the services provided to the identified Customer.
- The duration of such contracts.
- The volume of services, and the quality of services provided.
- The size and scope of each contract used as a reference.

Describe any important similarities or differences between the listed contracts and the services to be performed under MFN-3.

2.2.6 Business Qualifications

This information is intended to provide details related to business qualifications related to the overall MFN-3 services and service delivery.

Provide the following:

- A concise summary that provides essential information about the Respondent and subcontractor business and the relationship with subcontractors, subsidiaries, parent corporations, affiliates, and other related companies.
- Organization charts and a description of the governance structure and details concerning any pre-existing facilities that serve the Florida market.
- Organizational charts and define the relationship between the subcontractor[s] and the Services Provider. Include information such as market position, market penetration, and other business fundamentals within the telecommunications industry.
- A description of the historic experience the Services Provider has managing subcontractors.

2.3 General Requirements

2.3.1 Use of Manufacturer's Descriptive Text

Unless otherwise specified, any manufacturers' names, trade names, brand names, information, and/or catalog numbers listed in a specification are descriptive, not restrictive.

2.3.2 Subcontracting Requirements

Where subcontracting is permitted, only ~~direct~~ subcontractors of the service provider that have received the Department's prior written approval will be permitted to provide

services off of the contract. Contact information must be provided for each approved subcontractor so that the Department may reach out to the subcontractor directly. Subcontractors must be approved before beginning work on the Contract. At the Department's discretion, subcontractors may be added or removed from participation on the Contract at any time.

2.3.3 Flexibility to Quickly Modify Services

The Services Provider must manage change in a timely fashion. The ability to tailor the MFN-3 Enterprise is a critical design consideration, and changes and modifications may need to be made quickly. These changes and modifications may be made to the contract if within the general scope of MFN-3 services.

Outline how administrative, technical, and component level flexibility will be provided for the items listed below and other aspects of MFN-3.

Administrative flexibility should provide simplicity when adopting new features and assessment of SLA credits.

Technical flexibility should permit DMS control over maintenance windows and activities such as code upgrades and OS patching.

The various technical implementations should facilitate SLA monitoring, measurement, and scrubbing. Implementations should permit flexibility to quickly update a variety of hardware and software components.

Tools should work at the Enterprise level and permit granularity down to the Customer and individual site level for measurement and reporting.

The Contractor shall promptly modify functionality, as directed by DMS at DMS' sole discretion, in real-time to mitigate network performance concerns.

The Contractor shall promptly modify security related functionality, as directed by DMS at DMS' sole discretion, in real-time to make changes as needed to react to or investigate security events.

2.3.4 Service Testing Requirements

Vendor must test services and equipment before deployment to validate routing, switching, failover, and all current SLAs are going to be met during production to ensure production readiness.

DMS requires the Vendor to provide compute power and images (Network Operating Systems - NOS) throughout the duration of contract for testing purposes.

At no cost and at the request of DMS, the Services Provider shall provide DMS a CPE (with any feature set) for testing purposes.

2.3.5 Operational and Contractual Oversight Role

The role of DMS staff is to provide operational and contractual oversight and provides final decision on all contract and oversight decisions related to this contract and services. The role of DMS in operational and contractual oversight is critical. The Services Provider must facilitate DMS carrying out activities related to its oversight role.

2.3.6 Training on MFN-3 Technologies, Tools, and Services

DMS staff members will require training in order to maintain expertise with communications systems, services, and tools as it relates to MFN-3. Training sessions will be essential for DMS staff and Customers. The Services Provider will provide trainings at no cost to DMS staff and Customers to establish and maintain expertise with communications systems, services, and tools as it relates to MFN-3. The trainings will consist of network and security architecture, and the MFN-3 tools suite. The frequencies and logistics for this type of training will be coordinated with the Customer and DMS. Additional trainings and frequencies may be added at the request of DMS.

Instructors must possess advanced knowledge and experience on the topic they present. Instructors can be from the Contractor's and subcontractor's teams. While training will often be conducted remotely, in-person training must be provided upon request by DMS.

2.3.7 Administrative Support and Technical Refresh

The Services Provider must commit to an ongoing refresh process for the life of the Contract as an inherent feature of MFN-3 with no extra cost to DMS or its Customers.

Describe the proposed administrative support and technical refresh process that incorporates the following. The refresh process is to span all MFN-3 components (e.g., core infrastructure, daily operations, tools, billing, NOC, hardware, software, security, monitoring, etc.). Refresh will take place at the appropriate time to ensure completion of replacement prior to ~~EOL~~EOS. Refresh will commence as needed to ensure all MFN-3 service levels are continually met, that full Services Provider and Original Equipment Manufacturer (OEM) support is continuously available, and DMS receives new features in a timely fashion. Refresh is needed to mitigate software dependency challenges for MFN-3 Customers that would affect their ability to use MFN-3 tools or ability to migrate to a new application due to interdependencies. All features and functionality will be supported completely for the initial term and any renewal term of the contract. The MFN-3 Network and CPE software suite will be refreshed to newer versions based on software quality and longevity, as long as the result will not have an undesirable impact on DMS or its Customers. While standard CPE packages proposed in the **Attachment G, Instructions for Cost Reply Price Workbook** (Cost Reply), are to be finalized in the contract development process and as part of Certified CPE List updates, equivalent functionality will be maintained for the life of the MFN-3 service; the Certified CPE List will evolve. Administrative and technical support within the Services provider's organization is required for numerous MFN-3 related tasks. For refresh, these support requirements include project management tasks related to field-refresh services to address CPE change-out. Field refresh shall be accomplished to meet DMS, Customer and SLA requirements. Project management and field support resources will be augmented to meet these normal, but infrequent, change-out tasks. For CPE under maintenance, software and hardware refresh will occur to rectify a bug causing a service impact, rectify a security vulnerability or zero-day exploit of software/firmware even if the CPE is not ~~EOL~~EOS, support any new service which requires a new feature and ensure full Services provider support from the CPE

manufacture. Each scenario will be handled by the Department based on specific needs and requirements.

Include charts and other descriptive information to provide the following:

- Proposed timeframes for meeting the refresh requirements.
- In the proposed refresh process define the strategy, including a specific timeframe, for providing upgrades once equipment is declared end-of-support by the OEM; and address upgrading all equipment (hardware and software) before the end-of-support deadlines declared by the OEM. There is an SLA associated with this requirement described in **Attachment C, Service Level Agreements**.
- In the refresh process, outline how to deal with the need to augment both project and field staff to address change-out tasks.

2.3.8 Support for Team Collaboration Tool

DMS and the Services Provider's team will often collaborate on documents and services. Under MFN-2, DMS uses OwnCloud as the Collaboration Tool for sharing documents. Any future collaboration tool would be expected to provide comparable features as our existing tool.

Define the functionality of a Services Provider-provided system to support team collaboration, including document sharing.

2.3.9 Inspection Process

Per DMS discretion, inspections will be conducted to verify that MFN-3 components and services are being provided in accordance with the Contract. Seven (7) business days written notice will be given by the Department to the Services Provider prior to the inspection. The inspection process requires DMS staff to visit facilities housing MFN-3 services. DMS will use an inspection checklist when conducting inspections.

Provide a proposed checklist for inspection of facilities where infrastructure services such as the MFN-3 Core Network, the Internet gateway, NOC/SOC, and NMS tools are located. Also provide a proposed MFN-3 inspection process.

2.3.10 Logging by Default

The Services Provider will make logging the default. All services capable of logging are required to do so.

Provide a list of any logging limitations for MFN-3

2.3.11 Operational Meetings

A critical component will be frequent meetings with the Services Provider and its subcontractors to discuss the network and all its services. Meetings cover a review of operational concerns (review of NOC tickets), technical updates/changes, and as needed administrative topics. While there will be discussions on current and future services, these meetings are not sales meetings. Discussions will be held at the location and manner of DMS' choosing, and appropriate engineering staff representing the Services Provider and its sub-contractors shall be required to attend.

Technical meetings will take place at a minimum of bi-weekly, subject to change at the Department's discretion, to discuss engineering, design, and related concerns.

Security related operational and policy matters are expected to be addressed in a similar bi-weekly meeting. Meetings must cover ongoing service tuning including updates to attack signatures, thresholds, hardware, software, and procedures.

A Customer and management focused monthly operations meeting will also be held, to include the outcome of the SLA scrubbing process.

The Services Provider is responsible for the business (administrative) tasks associated with each of these meetings; agenda development, meeting minutes, and other meeting planning efforts. All SLAs within **Attachment C, Service Level Agreements** must be covered within the monthly operational reviews, including SLAs governing timely service outage notifications and simple CPE configuration changes.

2.3.12 Surcharges and Fees

The Services Provider shall not be permitted to charge for surcharges, fees, or taxes included but not limited to Universal Services Fund Fees. The Department will provide applicable tax-exemption documentation when requested.

2.3.13 Naming Conventions

To promote a simple-to-use structure, the Services Provider will work with DMS to develop a naming convention for all services offered under MFN-3. The naming convention includes but is not limited to device names, interface descriptions, comments, banners, groups, rule names, policy names, etc. System and device names must be registered and used within DNS.

A Unique Service Identifier USI is used as an intelligent name for NOC monitoring. example: MFN-DHSMV-BNNL-01. (MFN)=Vendor (DHSMV)=state agency (BNNL)=city (01)=circuit sequence.

2.3.14 Network Time Service

Interoperability, network/physical security, regulatory standards, and best practices require time synchronization. DMS requires two geographically separated network time servers delivering micro-second timing to mission critical systems. In addition to all MyFloridaNet-3 devices, other Enterprise services and critical applications (e.g. E911 statewide ESINet) shall be able to poll both network time servers. Customers shall have access to these servers to obtain network time. All Services Provider-provided systems shall utilize these servers. The time is true UTC (uncorrected for region). Configuration for Network Time Service is part of the standard MFN templates and is provided to Customer-managed agencies.

Time stamps must be used by network devices and tools to notate events which are critical to troubleshooting and MFN-3 SLA measurements.

Provide details on how this Network Time Service will be implemented addressing at a minimum the points above. How will you ensure that there will be an accurate standard time across all network services?

2.3.15 Continuity of Operations Plan

Provide a detailed Continuity of Operations Plan (COOP) and a process for updating the COOP before any sites migrate to the production core. The plan will be used in conjunction with staffing material to provide DMS with an understanding of how well the Respondent recognizes the scope and complexity of the MyFloridaNet-3 Enterprise requirements. The COOP's defined failover testing plan shall include all dedicated core services including core nodes, IAG, Internet access, Centralized VPN service, NOC/SOC, NMS tools, and any other core component that is listed as redundant. COOP plan must be reviewed annually by the Services Provider. Failover testing shall be performed annually for all components and services unless DMS waives this requirement during a specific year. Equipment and services will be physically powered down during failover testing. The Services Provider will produce detailed results based on the failover test and any remediation of issues discovered. No SLAs will be waived if a failover test results in outage bringing down sites or causing any performance degradation. Place the plan in the reply packet following the instructions provided in the ITN instructions Section 3.7 Contents of Reply/Reply Submission.

DMS requires the COOP to be developed by an individual/team with experience in continuity of operations planning. Indicate the level of experience for those responsible for the development of the COOP. That level of experience will be required for those updating the plan during the life of the Contract.

2.3.16 Growth Planning

As Customer requirements grow over the life of the Contract, the Services Provider is required to plan for and accommodate in advance the increasing needs of the MFN-3 Customer base for any MFN-3 Services Infrastructure at no additional cost to DMS or its Customers. There are no quantity commitments or revenue guarantees associated with any service provided under this Contract.

Describe the measurements and business processes that will be used to determine when scaling of people, processes, equipment, and other technology needs to take place.

Describe the proposed processes by which new equipment will be evaluated and introduced for inclusion in the MFN-3 Services Infrastructure.

2.3.17 Multi-Factor Authentication

This can be delivered either through a <u>dedicated or commercial solution</u>.

All components that can support Multi-Factor Authentication must provide Multi-Factor Authentication.

2.3.18 Vendor Access to Sites

Any physical site that is used to provide service to MFN-3 Customers shall use access procedures that require visitors to provide their U.S. or State Government-issued identification for verification by security. Access to sites by any vendor, subcontractor, or other visitors is to be digitally logged. Access logs must be made available to DMS upon request.

2.3.19 SUNCOM Service Integration

Proposed services are required to facilitate ordering of products from the catalog for delivering other SUNCOM services across the MFN-3 network.

2.4 Wide Area Network Enterprise Security Services

Services under this section are inherent to MFN-3 and should be bundled into existing service costs, so there is no specific entry within **Attachment K, Cost Reply Price Workbook**. The cost of services and operational functions that do not have a corresponding line on the price sheet must be spread across relevant, related components. The cost of the SIEM must be spread across all service components.

2.4.1 Enterprise Firewall

The acceptable delivery methodology for the Enterprise Firewall is dedicated only.

The services provided in this section by the Services provider may not be subcontracted and must be directly provided by the Services provider.

The Services Provider must provide Internet services combined with an Enterprise Firewall function to protect against unauthorized use and access. The MFN-3 firewall functions shall have the capability to be virtualized for multi-purpose contexts (e.g., Public VRF (OEU), Common Services VRF, or any internet facing VRF). As an Enterprise service applied on a statewide basis, it must use a uniform approach for the design and be supported by a suite of tools for use by the Services Provider, DMS, and Customers.

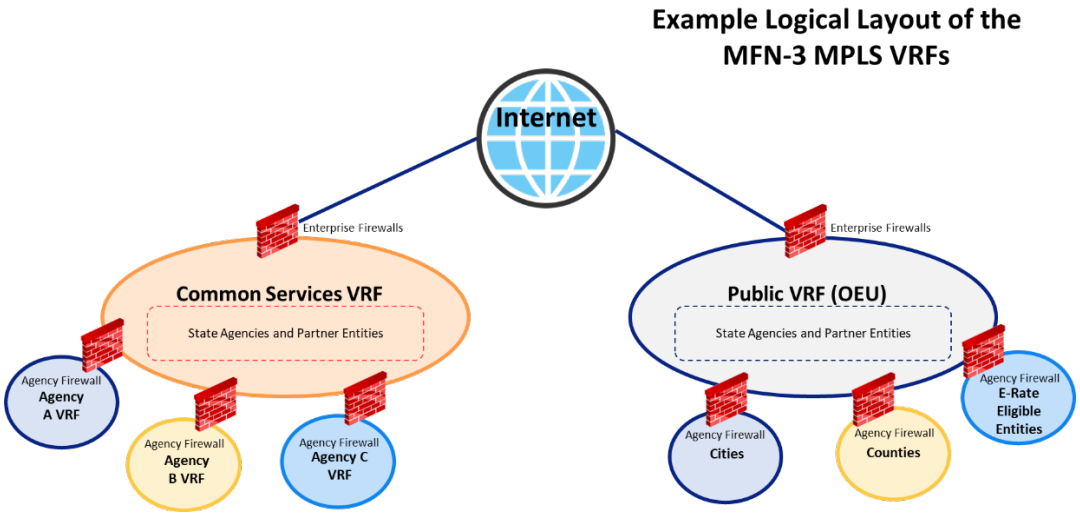


Figure 1 : Logical Layout of MFN-3 MPLS VRFs

The Enterprise Firewalls must establish a security perimeter and protect any Internet facing VRFs including but not limited to Common Services VRF, Public VRF (OEU), or any other routing domains. DMS at its sole discretion will utilize the Enterprise Firewall to fulfil its security requirements on MFN-3. This includes any features provided as part of the Enterprise Firewall platform.

DMS will work with Respondent to implement its security configurations for the different routing domains. In addition, any changes related to the security configurations of currently implemented routing domains shall be permitted.

The Respondent is required to deploy the Enterprise Firewalls in High Availability groups in geographically diverse Internet Access Gateway Complexes with a minimum node count of two Enterprise Firewalls per group.

DMS at its sole discretion will utilize the Enterprise Firewall to fulfil its security requirements on MFN-3. This includes any features provided as part of the Enterprise Firewall platform. Changes can be made at an Enterprise or IP address or Customer level.

Describe the overall architecture of the Enterprise Firewalls and include number of firewalls, location, and throughput capabilities with all functions enabled.

The Services Provider must provide and be responsible for the following activities:

- Ensuring optimal configuration, tuning, and providing management 24 hours a day, 7 days a week and 365 days a year (24x7x365).
- Monitoring services with well trained (certified) security experts.
- Providing firewall subscriptions that protects from network-borne threats.
- Firewall provisioning, deployment, upgrades, and patch management.
- Firewall backup and recovery (operating system and its configuration).
- Firewall configuration and signature management.
- Managing firewall's policy-based control over applications, end-users, and content.
- Directing all firewall logging to the Enterprise Security Information & Event Manager (SIEM).

Describe how these and other design criteria are addressed in the proposed Enterprise Firewall solution.

- All elements must be configured in a robust fashion since these components represent potential choke points for State services. All efforts must be taken to avoid any single point of failure.
- All components related to these features must be dedicated to the State network.
- DMS operational staff must have complete read-only access to all devices providing Internet protection to maintain a watch on service performance. Read-only access must include all management access protocols such as CLI via SSH, SNMP, GUI (HTTPS), API, FTPS, TFTP, RDP, etc. where available.

Describe how the Enterprise Firewall will provide the following security functions for all virtual contexts.

- Geo Blocking: Used to prevent network-based access to internal resources by blocking based on geographic location.
- Reputation-based Blocking: Used to prevent network-based access to internal resources by blocking based on a site's reputation as a malicious entity.

- Application Blocking: Used to identify and block unwanted applications without regard to the port they are using for communication.
- IPS & IDS: By proactively applying deep packet and application inspection of network activity at the edge of the network, and on the internally protected zones, these services will provide better analysis and overall security. Automated Correlation and Intrusion Analysis by this service will provide notifications of suspected unauthorized network activity and has the ability to prevent the activity from ever reaching the Customer's internal network.
- Malware & Anti-Virus detection: This service feature provides real time anti-virus and anti-malware protection. The Services provider must have the ability to automatically take action on malicious files currently in transport across the network. This feature will block unwanted malware and viruses at MFN-3 edge devices before they consume Internet bandwidth or threaten the local network and ultimately desktop endpoint systems users depend on to access the Internet.

Describe how the Services Provider has implemented the functionality proposed in this subsection within at least one other network. If Services Provider has not implemented the functionality in another network, explain why it is being proposed and when it will be available for implementation.

2.4.2 General Description - Operational Aspects of the Wide Area Network Enterprise Security Service

MFN-3 will have an Enterprise security service.

Describe the security logging functionality and security review strategies that will be made available to DMS, addressing the minimum requirements below:

Initial Setup and Configuration of Security Service Equipment Immediately Prior to Production (e.g. MFN-3 Enterprise Firewall): Prior to any Customer migrations to the MFN-3 infrastructure, the security system installation must be complete. Meetings between the Respondents security engineers, Security Operations Center (SOC), DMS, and Customers are required to define processes and make initial configuration determinations.

The installation process must include these administrative processes:

- Determination of how and when updates are to be applied.
- Specifying the (initial) detailed filters and the list of IP blocks protected.
- Establishing (initial) thresholds for different categories of alerts.
- Agreement on the matrix of alert levels and corresponding notifications including distribution lists.
- Development of an escalation process.
- Development of incident response procedures for attack categories and mitigation responses for the suite of threat concerns.

Ongoing Service Tuning: Ongoing service tuning must be provided by the Services Provider including but not limited to the following:

- Updates to attack signatures, thresholds, hardware, software, and procedures (day-to-day production implementation).

- Day-to-day maintenance of intrusion detection and mitigation equipment
- Backup and recovery (operating systems and configurations).
- Changes to systems and processes, for example, adjustments to thresholds for alerts.

Describe how the Services Provider has implemented the functionality proposed in this subsection within at least one other network. If Services Provider has not implemented the functionality in another network, explain why it is being proposed and when it will be available for implementation.

2.4.3 Security Operations Center (SOC)

DMS requires a centralized support unit on an organizational and technical level in the Services Provider's organization to deal only with security issues.

Describe how SOC functions will be made available to DMS, with the minimum requirements below.

- A facility located within the United States of America which is physically secured to permit entry of only authorized personnel, as determined by the Contractor.
- Geographically redundant SOCs must proactively monitor and protect network and data 24x7x365. The Services Provider's SOC facilities must operate in a carrier class facility with backup power, and redundant systems. The redundant system for tools must be housed in the geographically redundant facility.
- SOC must be staffed with certified, experienced, well-trained, and well-equipped professionals. SOC staff performs daily operational “eyes on glass” real-time monitoring and analysis of security events from multiple sources including but not limited to events from Security Information Event Monitoring tools, network-based intrusion detection systems, NetFlow, firewall logs, router logs, system logs, NMS tools and their supporting systems.
- Any network security component being managed must receive full monitoring support and the SOC must respond and assist effectively to mitigate any malicious threats 24x7x365. Customers must receive unlimited remediation support and consultation from security expert tiers at the SOC.
- There will be no limitation on the number of calls to the SOCs. The SOC will function as the point of contact for MyFloridaNet-3 users when placing the initial call for security related events.
- As part of their role securing the WAN Enterprise infrastructure, SOC staff must assist in identifying threats and developing preventative counter measures based on information collected from monitoring events worldwide. The team consists of cyber threat researchers that are assigned to the pursuit of existing and emerging global cyber threats. The team will research the global landscape, perform in-depth analysis of emerging threats, and develop counter measures to protect MyFloridaNet-3 Customers.
- SOC staff will have the ability to make security changes on-the-fly in response to proactive and reactive security concerns.

Describe how the Services Provider has implemented the functionality proposed in this subsection within at least one other network. If the Services Provider has not

implemented the functionality in another network, explain why it is being proposed and when it will be available for implementation.

2.4.4 Enterprise Security Information Event Manager Tool

This can be delivered either through a dedicated or commercial solution.

Provide an Enterprise Security Information & Event Management (SIEM) solution that provides log management, event management, reporting, and behavioral analysis for networks and applications. The SIEM functions as the tool the Services Provider, DMS, and Customers use to view security related information. DMS and each MFN-3 Customer shall receive as many accounts as required by the Customer.

Provide a description of how the SIEM functions will be provided. Include the following requirements:

- Customers must be provided a security product with a scalable database designed to capture real-time log event and network flow data, revealing the footprints of potential attackers.
- The SIEM must be implemented as an Enterprise solution that consolidates log source event data from thousands of devices distributed across the network, storing every activity in its raw form, and then performing immediate correlation activities on fields from differentiating source types to distinguish the real threats from false positives.
- The SIEM must capture and store real-time network flow data for search and analysis.
- The SIEM must have the capability to consolidate log source event data from devices endpoints distributed throughout MFN-3, which include but are not limited to:
    - Internet complex firewalls with unified threat prevention
    - MFN-3 core router system logs, and flows (IPFIX, NetFlow v9, J-flow)
    - If a commercial solution is proposed, all shared commercial components are not required to forward logs
    - MFN-3 CPE and firewall system logs, including both allow and deny logs
    - MFN-3 Managed Security Services logs
    - MFN-3 tools and their related systems
- Based on all the log source event data, the SIEM must perform immediate normalization and correlation activities on raw data to distinguish real threats from false positives. The solution must incorporate threat intelligence which supplies a list of potentially malicious IP addresses including malware hosts, spam sources, and other threats. The SIEM shall correlate system vulnerabilities with event and network data, helping to prioritize security incidents for each MyFloridaNet-3 Customer.
- The SIEM must provide near real-time visibility for threat detection and prioritization, delivering surveillance throughout the entire IT infrastructure.
- The SIEM must reduce and prioritize alerts to focus investigations on an actionable list of suspected incidents.

- The SIEM must enable more effective threat management while producing detailed data access and user activity reports.
- The Services Provider must identify and consistently group all Customer IP network addresses utilizing a naming convention that easily identifies the Customer and the network being private, common service, and public network.
- The SIEM must provide each Customer with a scope of view and command to their unique domain while DMS and the Services Provider must have an Enterprise view over all Customers.
- Providing real-time visibility and reporting of security events and associated incidents.
- Like pieces of metadata ingested into the SIEM must be normalized across indexed fields. (e.g. Source address from flow record and source address from log record mapped to “sourceaddress”)
- The SIEM must monitor events from all MFN-3 network components including MFN-3 tool suite components.

Describe how the Services Provider has implemented the functionality proposed in this subsection within at least one other network and indicate the size and scope of the other network. If the Services Provider has not implemented the functionality in another network, explain why it is being proposed and when it will be available for implementation.

2.4.5 Authentication Service

This can be offered as <u>commercial or dedicated</u>.

Where dedicated, all MFN-3 network devices (including core and Internet equipment), security devices, and any network-related and tools servers shall support multi-factor authentication (MFA).

Provide a description of how the Authentication Service functionality will be made available to DMS addressing at a minimum, the points below:

- During the development of the MFN-3 Services Infrastructure Build-out Plan, the respective teams shall discuss the required implementation of password protection for access to MFN-3 core components
- The authentication service shall support encryption and the authentication service itself shall log to the MFN-3 Enterprise SIEM. The reply must indicate the encryption scheme.
- The authentication service shall have the option of including passcodes comprised of up to eight characters using a selectable combination of digits, upper- and lower-case letters, and punctuation.
- Password and other user authentication changes across all services and tools shall be accessible through a self-service portal.

2.4.6 Assisting DMS in its Efforts Related to Security Compliance Audits, Training, and Awareness

Currently, Customers are responsible for their security for both hardware and software products used. Under MyFloridaNet-3 there is no requirement for the Services Provider to take over the Customer LAN data security for any location. Each of the

Customers will purchase hardware and software as needed to provide a level of data security consistent with their business policies.

However, the Services Provider providing the MFN-3 WAN Enterprise Infrastructure must assist DMS in its efforts related to WAN security. The Services Provider will assist DMS in its efforts to respond to various security compliance audits, training & awareness, policy development, as well as the development of best practices.

2.4.7 Operational and Security Review of Logs and Interpretation of Traffic Flows

When there is a networking concern, either operational or security, the Services Provider must provide active assistance reviewing logs and interpreting traffic flows.

2.4.8 Security Logging Functionality and Review Strategies

A critical component of MyFloridaNet-3 security will be ongoing security monitoring, both automated and manual. Dedicated equipment within MyFloridaNet-3 must be able to provide log files which can be reviewed by the Services Provider and DMS.

Describe in detail the tools, personnel resources, and monitoring processes that will be used to implement, maintain, and monitor security, the ongoing security monitoring functions for the Services Provider's infrastructure and Customer sites and the security logging functionality and review strategies.

2.4.9 Proactive and Reactive Security

MyFloridaNet-3 will address security threats originating within the State intranet as well as from the Internet and be both proactive and reactive for both intranet and external connections.

SOC personnel shall monitor "eye-on-glass" all core-to-core and Internet gateway traffic 24x7x365. Upon receipt or detection of a Qualifying Alert or upon active verification by SOC personnel of a suspected or actual cyber-attack, the Services Provider shall open an incident ticket and notify the Customer and DMS NOC within 15 minutes of the Services Provider's receipt or detection of such Qualifying Alert or verified activity and shall track the event through the mitigation process.

For purposes of this section, a "Qualifying Alert" means, at a minimum, any security alert, event, or combination of events identified by an in-scope security monitoring, detection, prevention, or network security device or system that:

(a) is assigned a High or Critical severity by the applicable security device, platform, or monitoring system;

(b) provides a credible indication of an actual or attempted compromise of the confidentiality, integrity, or availability of DMS or Customer information systems, networks, services, or data;

(c) indicates or reasonably suggests unauthorized access, privilege escalation, credential compromise, malware or ransomware activity, command-and-control communications, exploitation or attempted exploitation of a vulnerability, lateral movement, data exfiltration, denial-of-service activity, unauthorized security-control changes, or other malicious activity;

(d) is identified by the Services Provider SOC personnel, through active monitoring, analysis, correlation, or investigation, as reasonably indicative of a cybersecurity incident or an attempted cybersecurity incident; or

(e) is otherwise reasonably determined by DMS to present a material or potentially material cybersecurity threat to the DMS or Customer environment.

For the avoidance of doubt, an alert shall not cease to be a Qualifying Alert solely because the Services Provider subsequently determines that the alert may be a false positive, provided that the alert otherwise satisfied one or more of the foregoing criteria at the time it was received or detected. The Services Provider may subsequently classify an alert as a false positive or otherwise non-reportable following investigation, but such determination shall not relieve the Services Provider of the obligation to provide the notification required by this section when the applicable Qualifying Alert criteria were initially satisfied.

Within thirty (30) days following execution of the Contract, DMS and the Services Provider shall establish a written Qualifying Alert Matrix identifying applicable alert types, severity levels, detection sources, escalation criteria, and reporting procedures. The Qualifying Alert Matrix may supplement and provide greater specificity to the requirements of this section, but shall not eliminate, narrow, or otherwise reduce the minimum definition of a Qualifying Alert established herein unless expressly authorized by a written amendment to this Contract.

DMS shall have final authority to determine whether an alert or event constitutes a Qualifying Alert for purposes of the Services Provider's obligations under the Contract; provided, however, that Services Provider shall comply with the minimum requirements of this section regardless of whether the Qualifying Alert Matrix has been finalized or subsequently amended. There is an SLA related to Security Incident Identification.

The Services Provider is required to provide a weekly report that identifies the number and type of security alerts received or detected, the number reported as Qualifying Alerts, and the disposition of alerts not reported as Qualifying Alerts. The report shall provide sufficient information to justify why each material category of alerts was not deemed reportable. For example, if there are a total of fifty (50) alerts in a day and only ten (10) are reported, the weekly report shall identify and explain the basis upon which the remaining forty (40) alerts were determined not to be Qualifying Alerts.

The Services Provider shall not suppress, disable, downgrade, or otherwise modify the severity or reporting treatment of a security alert for the purpose or effect of avoiding the notification requirements of this section. If the Services Provider determines that excessive alert volume requires adjustment to alert thresholds, correlation rules, or other monitoring configurations, the Services Provider shall promptly notify DMS and initiate a discussion regarding such adjustment. No material reduction in the categories or severity of alerts subject to mandatory notification under this section shall be implemented without DMS's prior written approval.

A conference bridge may be established by the SOC and used during the mitigation process. If a reportable security notification is sent after hours, the SOC must follow

up with the appropriate Customer and DMS NOC personnel on the next working day regarding the status and disposition of the event.

Provide a description of how Respondent proposes to meet these requirements.

2.4.10 Denial of Service and Distributed Denial of Service Protection

This can be offered as <u>commercial or dedicated</u>.

DDoS attack must be mitigated using Cloud based DDoS scrubbing services, premises-based DDoS scrubbing services, or a combination thereof. The proposed solution should be able to scrub down to a host length prefix (/32 or /128). If a component of the proposed solution is premises-based, it must be deployed geographically at the IAG complexes and be dedicated to MFN-3.

DoS and DDoS protection shall be included and enabled for any Customer subscribing to MFN-3 Internet access services. The service will collect and monitor IP flow data to alert on traffic anomalies and attacks on IP addresses. The Respondent's solution shall protect MFN-3 Internet gateway circuits against network layer 3, 4, and 7 attacks. Denial of Service mitigation is a fully managed service; therefore, the Services Provider is responsible for all service functions. Through automated and manual processes, the Contractor is responsible for detecting potential concerns, determining when an attack has subsided, when mitigation processes are complete and reverting configuration changes to return the network to a normal posture. Due to the nature of protocol/application attacks and the increased risks associated with false positive traffic determination and the associated negative impacts on business processes, it is expected that the provided DDoS mitigation solution will support customized application of "features" on a per event/target basis permitting tuning of the response as required to mitigate the attack while also supporting legitimate flows.

The Services Provider will be responsible for the general functionality and processes listed below:

- Initial setup and configuration of DoS equipment (immediately prior to production)
- Ongoing service tuning (day-to-day production implementation)
- Identifying and fixing configuration errors
- Change management processes
- Developing the operational escalation process
- Providing real-time access to a robust reporting dashboard
- Define incident response procedures
- Host post-event operational meetings
- Test Cloud based mitigation on an annual basis

Describe how the Services Provider has implemented the functionality proposed in this subsection within at least one other network. If the Services Provider has not implemented the functionality in another network, explain why it is being proposed and when it will be available for implementation.

Include a detailed description of how the proposed service provides robust DoS and DDoS functionality. Include diagrams as necessary with the response or as an attachment.

2.4.11 Attack Types

The service will detect volumetric and application-based attacks.

Provide a detailed description of how the system detects attack profiles similar to the list below:

- DoS attacks (TCP, UDP, ICMP, Spoofed SYN flood, Non-Spoofed SYN flood, UDP flood, FIN, SYNACK flood, PING flood, Smurf or combined UDP/TCP/ICMP flood
- Fragmentation attacks such as IP/UDP, IP/ICMP, IP/TCP
- HTTP attacks such as connection floods, HTTP GET errors, HTTP suspended state
- BGP attacks
- DNS attacks

Describe advanced feature capabilities of the proposed solution to handle new attack profiles and adaptions. In addition, provide details on how the solution leverages available mitigation intelligence from CISA and other sources for customization and continuous improvement from a threat detection and mitigation perspective.

2.4.12 Individual IP Address Granularity and Maintaining Those Addresses

The Services Provider shall be responsible for obtaining and maintaining the list of addresses to be protected. If an IP address is the target of an attack, the Services Provider will send the notifications to the email address tied to the protected IP address.

2.4.13 Denial of Service Customer Profile

DMS is aware it will need to work with the Services Provider to develop Customer profiles to assist the Services Provider in management of the DoS service. It is likely that MFN-3 Customers will have traffic patterns that will, under normal circumstances, spike from time-to-time, and those spikes would not represent a DoS attack. It may be possible for DMS and the Services Provider to use a Customer profile and the IP Address Management tool as a resource in managing DoS service functionality. It may be possible for the Services Provider to use the Customer profile to identify addresses that are prone to attack or prone to spikes.

2.4.14 Real-time Access to a Robust Reporting Dashboard (Customer Portal)

The sophistication of any DoS (and DDoS) service is not solely based on how well it identifies an attack profile. DMS recognizes the effectiveness of the dashboard is critical as a tool for remediating an attack. The Services Provider will be required to provide the SOC, DMS and Customers with real-time access to a robust reporting dashboard (Customer portal) showing attacks and related statistical representations

of system functionality. Views and reports must include real-time and historical information. The general requirement is that a common system will serve the SOC, DMS, and the Customer.

Provide a detailed description of how the dashboard can display the needed information in a fashion appropriate to the incident and adapted to the level of technical detail useful to the individual.

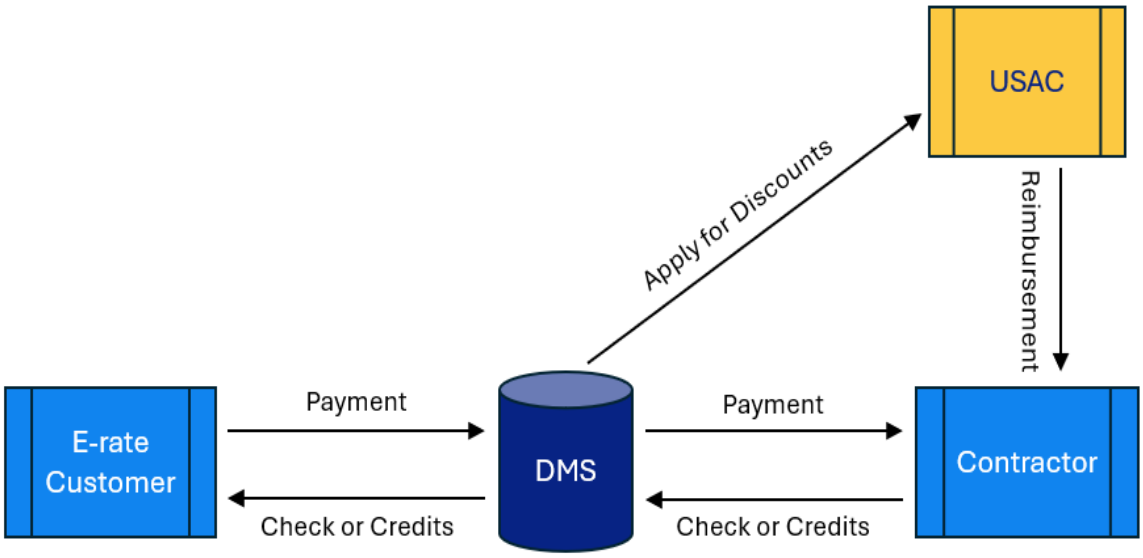
2.5 Universal Service Fund

2.5.1 Universal Service Fund Introduction

The Schools and Libraries Program of the Federal Universal Service Fund (USF), commonly known as "E-rate," is administered by the Universal Service Administrative Company (USAC), through its Schools and Libraries Division (SLD), under the direction of the Federal Communications Commission (FCC). The program provides discounts to assist eligible K-12 schools and libraries in obtaining eligible telecommunication services, telecommunications, Internet access, internal connections, and internal connections maintenance as defined in the annually published Eligible Services List.

E-rate rules and regulations (see https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-54 and https://docs.fcc.gov/public/attachments/FCC-10-175A1.pdf) require the entity that pays Vendors for E-rate eligible services and/or equipment on behalf of E-rate eligible schools and libraries (the “Billed Entity”) to be the E-rate Applicant for those services. Because the Department will pay the Contractor for services delivered to E-rate eligible schools and libraries under this Contract, the Department will be the Applicant for E-rate discounts for those services. If the Contractor is providing E- rate eligible services and/or equipment to the Department’s E-rate eligible Customers under the Contract, the Contractor shall meet the requirements in this section.

The Business Operations section of the Contract shall apply to any service provided to E-rate eligible Customers under the Contract. A brief overview of the Department E-rate process is shown below:



If the Contractor's authorized resellers or authorized dealers will provide one or more of the Contractor's requirements set forth in this Contract, that authorized reseller or authorized dealer will assume the obligations of the Contractor for this section. In that event, the Contractor will ensure that the authorized reseller or authorized dealer is in compliance with the obligations of this section.

To be eligible to provide services or equipment to E-rate eligible Customers under this Contract, the Contractor must have obtained or applied to obtain a Service Provider Identification Number (SPIN) from USAC prior to execution of the Contract and shall provide relevant SPIN(s) to the Department. The Contractor also is required to submit a Service Provider Annual Certification (SPAC) (Form 473) to USAC each funding year to certify that it will comply with E-rate rules and regulations. The Contractor shall maintain eligibility as an E-rate Service Provider under FCC rules and shall avoid being placed on "Red Light" status by the FCC for the duration of the Contract.

During the term of the Contract, the Contractor shall be required to take all appropriate action to provide eligible services and/or equipment in compliance with the terms and conditions of the Contract and E-rate rules and regulations. If the Contractor becomes ineligible as an E-rate Service Provider during the term of the Contract or becomes unwilling or unable to provide E-rate eligible services and/or equipment in compliance with the Contract and E-rate rules and regulations, the Department may seek to change to another E-rate Contractor and, if applicable, seek substitute services and/or equipment in accordance with applicable E-rate rules and procedures. See https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-54 and https://docs.fcc.gov/public/attachments/FCC-10-175A1.pdf.

If during the term of the Contract, the Contractor becomes ineligible as an E-rate Service Provider, becomes unwilling or unable to provide E-rate eligible services and/or equipment in compliance with E-rate rules and regulations or the Contract, or violates E-rate rules and regulations in a way that causes USAC to deny funding for Department applications on behalf of its E-Rate eligible Customers, in whole or in part, the following shall apply with respect to any ongoing E-Rate eligible projects:

The Contractor shall be liable for the actual direct damages incurred by the Department and any affected E-rate Customers that have complied with applicable E-rate rules and regulations as described in the paragraphs below.

In the event that the Department and its E-rate Customers change Contractors and seek substitute services and/or equipment pursuant to the above paragraph, direct damages shall include, but are not limited to, any amounts paid to the substituted Contractor above the Contractor's price under this Contract for the terminated services. The Contractor shall continue to provide the affected services and/or equipment to the Department and any affected E-rate Customers until such time as the Department and any affected E-rate Customers obtain substitute equipment as set forth above. In the event the Department or such E-rate Customers are unable to obtain USAC approval to change to a new Contractor because the Contractor's actions are deemed insufficient reason for approving a change of service providers under E-rate rules, the Contractor will be liable for the amount of E-rate funding forfeited as a result.

If the Contractor's violation of the E-rate rules and regulations is the reason for the Department and its E-rate Customers' loss or forfeiture of E-rate funding, in whole or in part, the value of the lost funding associated with the Contractor's violation will be considered a direct damage under this subparagraph 1.

The Department acknowledges that it has posted an E-rate Form 470 ("Description of Services Requested and Certification Form") in connection with the procurement, which is a prerequisite to E-rate eligible entities utilizing the Contract awarded as a result of the procurement as the basis for E-rate funding applications.

Additionally, the Department acknowledges that some E-rate Customers may post their own Form 470 and evaluate this Contract as a bid response to that Form 470.

Both the Contractor and the Department agree to the following:

E-rate has specific rules and regulations regarding, among other things, eligibility of services and/or equipment, the manner and timeframes under which USAC and SLD approve funding requests and distributions, the submission of FCC forms and related documentation, document retention and audits in connection with funding under the E-rate program.

In order to ensure that the billing mechanisms and processes established pursuant to this Contract with respect to the applications for discounts under the E-rate program are in compliance with E-rate requirements and regulations, the duties and responsibilities of each party and the format and content of invoices to the Department are set forth in the Business Operations section of the Contract.

The Contractor will provide such assistance as the Department and E-rate Customers deem reasonable with respect to information needed to accurately and timely complete E-rate forms and respond to USAC inquiries regarding the services and/or equipment provided herein.

The Contractor will comply with all E-rate rules pertaining to document retention and will make available to the Department any such documentation upon request.

In the event of an audit or review by USAC, the FCC, or any other entity of E-rate compliance related to this Contract, the Contractor agrees to provide all assistance, information and documentation requested by the Department to satisfy the audit or review.

Both Parties agree that the Contractor shall not be deemed a consultant of the Department or its E-rate eligible Customers.

2.5.2 Maintaining Florida's E-rate Eligibility under MyFloridaNet-3

DMS's paramount concern for this solicitation is to ensure that the selected Services Provider and any subcontractors, as well as all E-rate eligible services offered to K-12 schools and libraries, comply with E-rate rules and regulations. Accordingly, MFN-3's procurement, network design specifications, and service provision requirements must comply with FCC E-rate rules and USAC guidelines for eligibility.

DMS procures services through competitive bidding procedures. MyFloridaNet-3 Services shall be a state master contract, available to all local and state government entities, eligible non-profits, and private entities that perform functions for Florida governmental entities.

The Respondent shall comply with the requirements of the published 2026 Schools and Libraries Eligible Services List for Funding Year 2026, titled: Modernizing the E-Rate Program for Schools and Libraries, Eligible Services List, WC Docket No. 13-184, Released: December 17, 2025, (https://www.usac.org/e-rate/applicant-process/before-you-begin/eligible-services-list/) and subsequent editions as it pertains to the provision of all E-rate eligible services offered as a result of this procurement.

2.5.3 Services Provider's Liability for Maintaining Eligibility as a USF Service Provider

The Services Provider must maintain eligibility as a USF service provider and must not be placed on "Red Light Status" by the FCC or placed on the Suspension and Debarment List of the USAC. (See http://www.usac.org/sl/about/program-integrity/suspensions-debarments.aspx). The Services Provider must not be on "Red Light Status" by the FCC at the time of submittal of the response to this ITN. The Services Provider must be in compliance with FCC E-rate Program rules and regulations at all times. In the event that the FCC or USAC determines that the Services Provider or a subcontractor has not acted in compliance with E-rate Program rules, it can result in denial of funding, reduction in funding, repayment of funding (a commitment adjustment), audit or other investigation, for which the Services Provider will take full responsibility and be liable to keep the Department whole.

2.5.4 Eligibility under the USF E-rate program

The Services Provider must obtain a Service Provider Identification Number (SPIN) from USAC. The Services Provider must submit a Service Provider Annual Certification (SPAC) (Form 473) to USAC each funding year to certify that it will comply with E-rate rules and regulations.

Provide SPIN number(s) and a copy of the most recent SPAC as evidence of current eligibility for both the Services Provider and each of its subcontractors. This

information shall be provided as part of Tab 8 per the ITN instructions; do not place the evidence of USF, program eligibility in reply to this subsection.

2.5.5 E-rate Experience

Provide a summary of experience in the E-rate program including the number of years in the program, the scope of services provided, and any other relevant information detailing experience in providing services on the scale requested in this ITN, for the Services Provider and each subcontractor. Provide also evidence of the Services Provider E-Rate expertise in the form of E-Rate subject matter expert staff and/or contracted consultant(s).

2.5.6 E-rate Customer Care

If necessary, the Services Provider is required to assist DMS with expertise on rules and processes related to Universal Service Fund matters. The Services Provider will keep current with the expertise on all rules pertaining to the USF program. Based on these rules and requirements, the Services Provider must provide DMS and its Customers any information and/or documentation needed to complete forms or respond to USAC and/or FCC inquiries or requests for information. The Services Provider's E-rate support personnel will serve as single points-of-contact for DMS and its Customers that have been approved for E-rate funding. In addition to assisting with special requests from DMS and its Customers, routine responsibilities of E-rate support personnel include, but are not limited to:

- Contacting DMS E-rate personnel after DMS's applications are approved for funding to advise them who to contact for assistance within the Services Provider's support group.
- Enabling DMS to provide discounts on Customer bills (when SPI form is used) or reimbursements to Customers (when BEAR form is used).
- Assisting DMS in providing information for completion of BEAR Forms if needed and promptly certifying BEAR forms after they are filed by DMS.

2.5.7 E-rate Billing

The Services Provider must provide billing assistance to generate additional breakdowns of charges on the Services Provider bills to DMS to enable identification of E-rate eligible costs per Customer. The Services Provider must provide the following on all bills to DMS:

- The Funding Request Number (FRN);
- Customer Identification: A recognizable legal name with an identifying code associated with that name and the entity's location;
- A recognizable legal name and address for the physical location where services are provided
- An itemized breakdown of eligible costs per Customer per FRN.

The Services Provider must relate approved FRN with the billing numbers in order to establish a monthly E-rate credit on the bill. Once funding has been approved, Contractor will credit previously billed non-discounted amounts and bill discounted amounts (SPI only) by month, inventory number, and SKU. The Customer must work

with DMS to reconcile any discrepancies in billing related to receipt and distribution of E-rate funds.

2.6 Business Operations-Requirements

2.6.1 General Description of the SUNCOM Business Model using Customer CSAB

DMS serves two Customer categories: 1) Customers required by Florida Statutes to use SUNCOM services; and 2) Other Eligible Users such as counties, cities, schools and libraries, and certain non-profit organizations.

SUNCOM's standard business model, as governed by Part III of chapter 282, Florida Statutes (F.S.), and chapter 60FF-2, Florida Administrative Code (F.A.C.), establishes DMS as an aggregator of Florida's public sector telecommunications purchases. From the Services Provider's perspective, this means that DMS is a single Customer for all SUNCOM services. This is achieved not only through enterprise bulk contracts, but DMS also centralizes, consolidates, and standardizes all SUNCOM ordering and billing through the CSAB. The Communications Service Authorization and Billing (CSAB) system is the ordering, billing, incident management, and inventory system referred to in Chapter 60FF-2, F.A.C., that the Services Provider will be required to utilize.

When SUNCOM Customers log-in to CSAB, they can perform the following functions related to all telecommunications service types and providers:

- Establish CSAB user access privileges;
- Manage billing accounts;
- Review a comprehensive list of contracted services;
- Place orders;
- View their entire telecommunications inventory with associated event histories and charges;
- Review invoices with detail charges; and
- Provide information for completion of DMS E-rate Form 471 (eligible K-12 schools and libraries only).

Using a single invoice with supporting detail in electronic files for each service type, vendors bill DMS monthly for services rendered to all SUNCOM Customers. The supporting details include auditable charges at the activity level under unique identifiers for each transaction (for metered services) and service account.

In addition to empowering SUNCOM Customers with self-service and establishing substantial cost controls, this model minimizes vendor risks associated with collecting payment on thousands of billing accounts, then settling billing disputes with some of them. This model also achieves significant economies of scale for all parties through substantial automation from a series of three named API/SFTP electronic transactions between DMS and its vendors.

However, all but two electronic transactions have manual equivalents in CSAB screens whereby vendors can manually input the data that would otherwise come from the transaction. All of the same business rules apply (regarding timeliness, for example). Vendor use of these manual processes is less desirable as they require

data entry twice (once in the vendor's system then again in CSAB) and are more likely to produce errors. DMS is not responsible for inputting the data on the Vendor's behalf.

2.6.2 Responsibilities of DMS and the Vendor in the SUNCOM Business Model

2.6.2.1 Flowchart of SUNCOM Business Process

Figure 2 below is a flow chart of functions to be implemented by DMS, its Customers and the Vendor. Note there are three named "API/SFTP" transactions that are described in more detail below. This flow chart/process is subject to change.

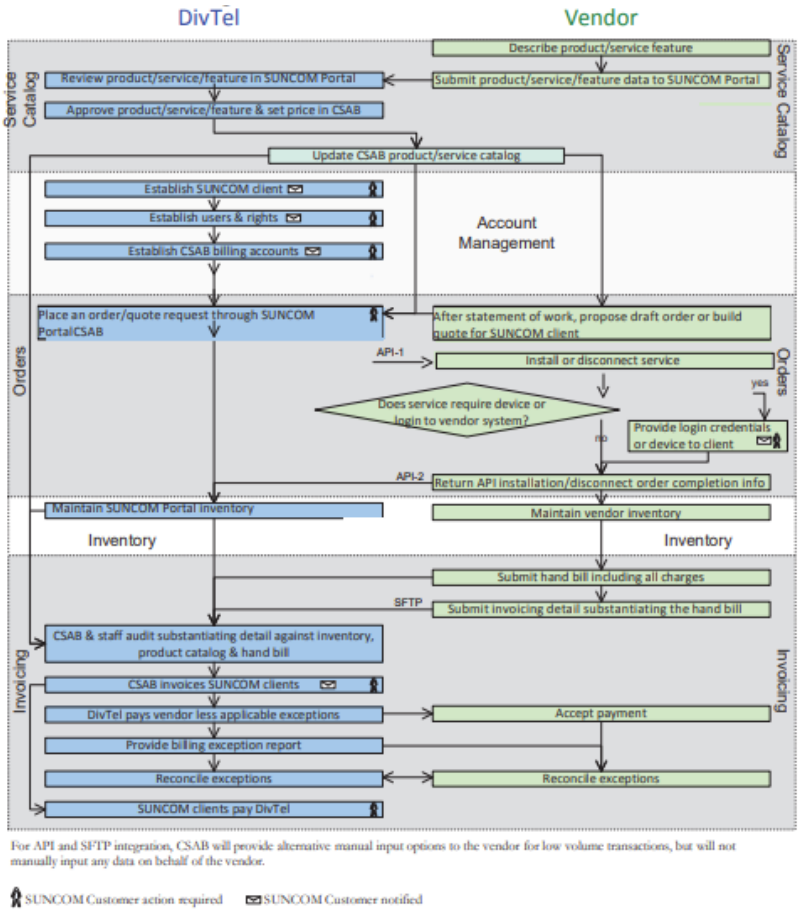


Figure 2: SUNCOM Business Process

2.6.2.2 CSAB – Official Record

There are no conditions where DMS staff or SUNCOM Customers will be required to manually use the Service Provider's systems to view, update, or extract order, billing, inventory, or account management data. These functions are exclusive to CSAB. If the Services Provider proposes to grant DMS or SUNCOM Customer access to its systems, DMS will consider it to be a supplemental offering that does not displace any

of the requirements described here for the vendor to exchange electronic data, or view and enter data into CSAB.

This policy, combined with the centralization and standardization of order processing and billing, means that CSAB is able to encompass all substantive data related to service accounts. Therefore, CSAB will be the official record of the inventory and costs of SUNCOM services. In reconciling billing disputes between the Customer and the Vendor, the CSAB data will be considered correct. The Services Provider must reflect service enhancements that have been made in CSAB. If inaccuracies are found within CSAB data, DMS will negotiate discrepancies in good faith and compensate vendors for services rendered in accordance with SUNCOM Customer CSAB orders.

2.6.3 CSAB Interfaces with Vendors

There are three primary ways to implement transactions between the DMS CSAB and the Vendor.

- Application Programming Interfaces:
  - APIs are defined here by five primary characteristics; 1) they are software routines initiated by a request from a business partner's system; 2) they accept data from that business partner and deliver data in return; 3) they perform these functions automatically upon demand at (near) real time; 4) interface procedures are defined and documented for business partners to use; and 5) they are followed by acknowledgements from the partner.
  - CSAB contains several APIs to facilitate Work Order-related transactions. API-1 transactions represent any Work Order-related transaction originating from CSAB and targeting a Services Provider's system. API-1 transactions may contain Work Order meta-data, including Customer contact information, location information, service features, due dates, etc. API-2 transactions represent any Work Order-related transaction originating from a Services provider's system and targeting CSAB. API-2 transactions may contain progress updates, work completion dates, effective billing dates, etc.
- Batch Routines:
  - Batch files are required for invoicing data substantiation (SFTP-1) Invoice substantiation files will be delivered monthly. Records within these batch files should include, at minimum, a unique Inventory identifier (preferably SUNCOM's Inventory ID), effective bill start and end dates, wholesale charge, quantity (instances, minutes, etc.), and rate identifier (tariff code, SKU, etc.).
- Manual Review and Data Entry by Vendor Staff:
  - Vendors can use CSAB screens to view a submitted order from a Customer and mark that order as fulfilled rather than use API-1 and API-2 transactions.
  - Neither DMS nor SUNCOM Customers will input data into CSAB on behalf of Vendors. In all instances where the Vendor is the source of data, the vendor must directly provide the data in CSAB. For example, the Vendor is required to verify that an order (submitted by the Customer) has

been fulfilled, and if the Vendor is unable to do so electronically with an API-2 transaction, it must input the fulfillment data directly into CSAB.
- For data that Vendor is not allowed to enter into CSAB, the Parties will work to ensure data completeness and accuracy.

2.6.4 Function Types in CSAB

2.6.4.1 Services Catalog

Relevant data regarding DMS-approved SUNCOM services and the relationships among them will be listed in the CSAB service catalog prior to making them available for use or purchase by any SUNCOM Customer. Even services which incur metered charges must be included in the catalog because DMS will require SUNCOM Customers to establish their rights to use metered services through an order prior to using them (i.e., ordering a metered service is an authorization to incur future metered charges).

Charge types are defined as:

- One-time charge: a single payment for a service or item, e.g. hardware installation.
- Subscription charge: monthly fixed and recurring charge for the right to use something without regard to how much it is used (such as local phone service).
- Metered charge: incremental charge based strictly on how much the service is used (such as long-distance phone minutes).

The CSAB system will hold corresponding catalog data of DMS authorized SUNCOM services. DMS will provide this data on services through direct data input.

DMS will submit data to be held in the CSAB catalog that indicates the relationships between services to ensure services ordered are compatible. For example, if a feature works with one service but not another (and it is not a part of a bundled package), the catalog must reflect this so the CSAB will preclude orders containing incompatible services.

As noted in section **2.3.12 "Surcharges and Fees,"** The Services Provider shall not be permitted to charge for surcharges, fees, or taxes included but not limited to Universal Services Fund Fees in the Services Catalog.

DMS's Sole Discretion over the Catalog

DMS will have sole discretion over whether or not the Services Provider's proposed services will be available for purchase in the CSAB catalog, and the prices charged to SUNCOM Customers for them (prices will include cost recovery fees to cover SUNCOM operations).

After the Services Provider submits the proposed description of services, the SUNCOM product manager will review for completeness and accuracy and for compliance with the contract and its scope. The SUNCOM product manager will also ensure that the proposed service offering fits within the portfolio of SUNCOM services and evaluate the cost value of the service and ensure the offering's consistency with DMS's statutory charge to offer services that are in the best public interest. If the

product manager authorizes a service, he/she will establish a price and make it available for purchase to SUNCOM Customers through CSAB.

If the SUNCOM product manager determines that a proposed service is not in the best interest of the Customer, it will not be made available for purchase through CSAB and DMS will not pay any charges associated with it. The SUNCOM product manager may determine that services previously provided are no longer in the best interest of MFN-3 Customers. DMS may remove approved services from CSAB at their sole discretion.

Unique circumstances exist where items can be purchased that do not appear in the catalog. Special construction, for example, may require non-standardized products. When orders or invoices contain such items, those items must be accurately priced and will require detailed analysis by SUNCOM engineers who must, ultimately, approve the transaction.

2.6.4.2 Account and User Management

SUNCOM User Access Privileges

Before buying SUNCOM services, new Customers will register in CSAB and agree to DMS terms and conditions. DMS staff will review these registrations to verify SUNCOM eligibility.

Once authorized to buy SUNCOM services, Customers will establish at least one, or any number, of CSAB billing account(s) that will correspond to distinct invoices where SUNCOM charges will accrue. Customers will also establish users with comprehensive or distinct authorities to draft and submit orders, view invoices and inventory, etc. These authorities can be specified at the billing account level or apply to the entire Customer. Customers can also grant users authority to order specific classes of services and establish catalog restrictions to prevent orders of certain services on a given account.

None of these Customer account and user management functions require any action from the Services Provider either in the vendor's system or CSAB.

Vendor User Access Privileges

User access privileges within CSAB must be approved and monitored by a Services Provider-assigned CSAB Administrator. User access privileges must be aligned with distinct job duties of the Services Provider staff. Based on assigned access privileges, the Services Provider staff may use CSAB for the following functions.

- Submit product/service/feature data description to DMS.
- Update order fulfillment data.
- Assist Customers by drafting orders that become vendor proposals in CSAB for Customers to later modify, submit, or delete. Review past orders submitted to the Services Provider.
- Review a robust set of inventory data for services provided by the Services Provider.
- DMS reserves the right to terminate the CSAB user access privileges of any Services Provider staff without cause or notice.

2.6.4.3 Orders

An authorized user of CSAB will be able to search and view services in the CSAB catalog and place orders for them under specific CSAB billing accounts. Customers can create orders in stages including drafts that can be routed to others for approval before officially placing an order. Upon completion, API-1 transactions will be sent to the Services Provider, or the Services Provider can log-on to CSAB, as prompted by a CSAB email, to see submitted orders.

From the perspective of the SUNCOM Customer, a single order may contain several items (services). Thus, the Services Provider will receive distinct "work orders" for each item. This allows for partial fulfillment of an order where appropriate (otherwise, multiple item orders with only a single order number cannot be fulfilled until every item is delivered). Therefore, Vendors are required to complete distinct fulfillment criteria, either manually or via an API-2 transaction, for each work order (item).

For data that Vendor is not allowed to enter into CSAB, the Parties will work to ensure data completeness and accuracy.

Some key data elements including but not limited to are:

- Order ID – identifies a request for one or more items. This ID is associated with everything in a "shopping cart" when a Customer "checks-out".
- Work Order ID – is associated with each item request within an Order that can be fulfilled separately from the rest of the Order.
- Price Code – identifies the service, feature or hardware from the Service Catalog that was requested in the Work Order.
- Service Installation ID – identifies an instance of a service resulting from Order fulfillment. It is the unique inventory entry in CSAB and is equivalent to, but not the same as, distinct IDs used by vendors to track status, usage and charges (e.g. circuit ID, phone number, hardware serial number, etc.).
- Physical Connection Type – identifies the physical connection type (i.e. fiber, copper, coaxial cable).
- Bandwidth – identifies the total capacity of the physical connection.
- Installation Start Date – The date the Services Provider will begin installation.
- Installation Date – The date the Services Provider will have completed installation.
- Service Start Date – The date the services will be turned on and available to the Customer.
- Effective Bill Date – The date on which charges will begin accruing.
- The FRN for E-rate supported services and components.
- Customer Identification - A recognizable legal name with an identifying code associated with that name and the entity's location.
- Location of Services - A recognizable legal name and address for the physical location where services are provided.
- Quantity – Number of items per SKU.

The Services Provider must provide all of the required fulfillment data in CSAB. While DMS strongly encourages providing automated fulfillment transactions to CSAB to prevent inaccuracies, delays and duplication of effort, CSAB provides a screen for the

Services Provider to manually update orders with fulfillment data as an alternative to electronic API-2 messages.

DMS cannot invoice its Customers without associating key fields from orders to SUNCOM Customer invoicing accounts in CSAB, and therefore will not pay for any services where such data is missing or incorrect. Installation and disconnect dates are also critical to the inventory as they are used during audits to verify that a service was active, or should not have been, during an invoicing period.

Some orders will include configuration data including IP addresses to enable establishing closed user groups on the State network.

Credential Request Orders

Some of the orders submitted to the Services Provider will request granting SUNCOM Customer password/PIN protected access to the Services Provider services. These are services that require Customers to log-in (or be electronically certified) to vendor systems before using a service. While a subscription charge might be associated with such orders (i.e. a monthly charge might be incurred for the right to use the account), it enables metered consumption of the associated service for which the right to access must first be ordered through CSAB. CSAB will be the exclusive source for orders requesting the right to access regardless of the cost, or lack thereof, associated with the service.

Like all other services, the right to access them will be ordered with API-1 transactions from CSAB providing the Services Provider with necessary data to enable that access. The Services Provider is expected to respond by confirming to CSAB that it has been provided. However, CSAB will not hold user passwords and PINs for access to the Services Provider systems thus the Services Provider is expected to provide them to users directly using email addresses provided in the CSAB order. PIN and password changes will be handled outside of CSAB, as well.

SUNCOM conferencing services are current examples of credential request orders. Users of the service must login to a vendor's system to reserve or initiate a conference. Thus, the vendor issues login credentials to those users that were obtained after an order for them (API-1) was placed in CSAB. The order is fulfilled by the vendor supplying a user ID and Personal Identification Number (PIN) via email to the user, then confirming fulfillment to CSAB with an API-2 transaction. These transactions enable CSAB to have a complete inventory of all of the users of the service. The vendor's system tracks usage that is attributable to each user, which is compiled in a SFTP monthly batch file of invoicing substantiation.

Figure 3: Credential Request Order Example

Special Construction Orders

Fulfilling some service requests under this Contract will require providing services not readily defined in the Service Catalog and/or require the Services Provider to

determine the quantity of cataloged services and/or propose a unique configuration. Examples include wiring installation at the Customer's site for which the amount of wiring and work to install it can only be determined after a site assessment by the Services Provider.

These are known as "special construction" orders.

As mentioned in Vendor Users & Rights, the Services Provider staff can draft orders to become the Services Provider proposals in CSAB for SUNCOM engineers and Customers to later modify, submit, or delete. This provides the mechanism for the Services Provider to make special construction proposals and for Customers to place the order. When a Customer has submitted an order drafted by a vendor, they have effectively accepted the vendor's proposal and authorized the work.

To the extent possible, special construction orders should name and quantify all of the services from the CSAB service catalog that will be used. But with some special construction, all of the hardware or services required might not be in the catalog.

With product manager approval, these services/hardware might be subsequently added to the catalog. But in all cases, the total cost of the proposed order must be defined and approved prior to submittal.

In addition to naming services to be provided, the order will contain other data necessary to specify and authorize the service like target installation dates, locations, configuration data and even documents containing diagrams where available.

There shall be no special construction charges for like-for-like bandwidth and media for sites being migrated from MFN-2 to MFN-3. The Service Provider is responsible for migration of Customers from these current services at no cost. Individual Customers are responsible for special construction costs after any migration to MFN-3.

2.6.4.4 Inventory

Inventory Record

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

CSAB inventory is structured around key data elements. No inventory record is valid without these key fields thus posing invoicing disputes when they are missing or inaccurate. And CSAB by default has primacy when there are discrepancies between the inventories of the Services Provider and CSAB.

2.6.4.5 Invoicing

Invoicing Requirements

The Services Provider will invoice DMS monthly for all SUNCOM services and fulfilled orders by service type. Invoices will consist of a single request for payment on unchangeable format known as a "hand bill" which reflects the total charges for the month, and electronic detail files that substantiate all billable services. The total of substantiated detail charges must match the single payment request on the handbill. Invoices for E-rate Customers must be submitted to DMS on a bill separate from other Customer billing.

Electronic Substantiating Detail File

The invoice substantiation file consists of ASCII delimited electronic detail listing all billable services and activities with all unique IDs necessary to be auditable bases for all charges. The detail file must include all charge data on one-time purchases, active subscription periods and metered incremental activities. All charges must be attributable to distinct identifiers from the service catalog, and each discrete metered charge must be distinguished by service account in CSAB. Metered charges must also include date/time stamps for each billing event.

DMS Response to Services provider Invoices

CSAB will pre-audit the invoice to match all charges against the current inventory of services provided and to the prices associated with the services in the catalog. Barring audit exceptions, DMS will pay the Services Provider the total charges on behalf of all SUNCOM Customers for all services rendered. If the electronic substantiating detail provided by the Services Provider contains some errors but is a) complete (i.e. contains all of the required data elements); b) substantially corresponds with the CSAB inventory and service catalog; and c) matches the hand bill, DMS will send an exception report to the Services Provider detailing any disputed charges. DMS staff will request credits for any exceptions and work with the Services Provider staff to reconcile charges and system data to resolve the exceptions.

The primary, but not exclusive, criteria for rejecting an invoice is found in answer to this question: does the substantiation file contain enough accurate detail information to enable DMS to clearly and accurately re-invoice its Customers? If not, DMS will notify the Services Provider of the dispute, reject the invoice, and request the Services Provider to submit a new invoice.

2.6.5 Access Ordering Process

For every access component order the following process must take place:

1. Customer places order in CSAB
2. Services Provider receives order
3. Services Provider determines whether there is a need to subcontract for any portion of the access order.
    a. If no, the Services Provider will create a quote for services based on the best price at the current market conditions, without exceeding contract prices
    b. If yes, the Services Provider sends the order to all approved Subcontractors. Subcontractors will provide a quote to the Service

Provider for services based on the best price at the current market conditions, without exceeding contract prices.

4. Services Provider returns the unaltered quote(s) to CSAB. Quote(s) must provide the best price based on the current market conditions, without exceeding contract prices.
5. Customer selects the quote that best meets their needs.

Quotes must be returned to the Customer within 10 calendar days

At a minimum, all quotes must include the following additional field requirements:

- Local loop carrier name
- Price
- Primary EVC circuit type declaration (Type I or Type II)
- Backup EVC circuit type declaration (Type I or Type II)

At a minimum, all Service Acceptance forms must include the following additional field requirements as part of the IMAC sign off process:

- Circuit ID
- PE Name (Primary and Backup)
- PE Location (Primary and Backup)
- Primary EVC circuit VLAN ID
- Backup EVC circuit VLAN ID

These pieces of data will be kept up to date in CSAB if service provisioning parameters change over the life of the service.

The access ordering process is subject to the Service Inquiry SLA in Attachment C.

2.6.6 Mandatory interface with CSAB

All work orders will be submitted to the Services Provider via the CSAB or similar system as deployed by DMS. Changes approved via NOC ticket and not impacting invoicing charges may be an exception.

2.6.7 Mandatory CSAB order

No site will be connected to MyFloridaNet-3 unless the Services Provider has a properly authorized work order submitted by DMS.

2.7 Core Functionality and Related Services

This can be delivered either through a <u>dedicated or commercial solution</u>.

The services provided in this section by the Services provider may not be subcontracted and must be directly provided by the Services provider.

2.7.1 General Core Services Infrastructure Requirements

The Services Provider is to comply with the following specific design requirements:

- DMS requires 99.99% availability and uptime for core resources. Vendor must ensure that the MFN-3 Core Services Infrastructure meets or exceeds all SLAs in Attachment C.
- All MFN-3 Core Services Infrastructure and offerings must not require downtime for upgrades, routine or anticipated maintenance. Individual components may have downtime for maintenance, but the system/service must remain operational and capable of properly supporting traffic.
- To promote a simple-to-use structure, the Services Provider will work with DMS to develop a naming convention.
- Where dedicated, MFN-3 core routers must not have interfaces directly exposed to the Internet (firewall service is required).
- For each site, a route-map must be defined on the Provider Edge router. The route-map must allow only the approved prefixes into the VRF as sanctioned by DMS.
- Core Services Infrastructure will not be referred to by their IP address, but rather through a hostname using DNS, with a standard naming convention that complies with MFN-3 naming conventions.
- The MFN-3 Core Services Infrastructure must support several techniques for multi-path load balancing which improves service offering capabilities.
- Fast Re-Route (FRR) or similar technology must be supported for all implementations to facilitate less than 200ms failover for core NNI link disruptions. Please explain how you will meet this SLA.
- For Customer-managed CPE, the MFN-3 core router must be capable of supporting inbound local packet marking or classification. For Services provider-managed CPE, the local packet marking must be done on the inbound LAN interface of the CPE router.
- The MFN-3 Core Services Infrastructure must support QoS for all access types.
- The MFN-3 Core Services Infrastructure must support the QoS classes below:

Table 1: QoS Class Types

Class	Forwarding Type
Voice	EF
Video	AF41
Application	AF21
Best Effort	BE
Signaling	AF31

Provide a detailed description of the proposed Core Services Infrastructure functionality, including, but not limited to, layout/design, standards to be used, location of POP sites, and any other attributes designed to meet the HA/HR needs for MFN-3 Core Services Infrastructure.

2.7.2 MFN-3 Core Services Infrastructure Build-out Plan

The Services Provider will be required to develop a detailed plan of the MFN-3 Core Services Infrastructure build-out. This plan will provide a detailed description of the requirements for the VRF connectivity as well as the network access and traffic routing requirements and considerations for all services and components such as core, access, multi-tenant, security and Internet connectivity.

2.7.3 Description of Proposed Virtual Routing and Forwarding (VRF) Structure(s)

Below are the different VRF types required on MFN-3; however, the Contract Service Provider must configure any additional VRFs at no additional cost based on DMS sole discretion. There shall be no limitations on the number of VRFs created on MFN-3. In addition, any changes to the current implemented VRFs shall be permitted.

- **Public VRF (Other Eligible Users):** This VRF is specific to Other Eligible Users (OEUs) including, but not limited to, cities, counties, non-profits, any educational or E-rate eligible entities. The Public routing domain on MFN-3 must be behind the Enterprise Firewall. At DMS's sole discretion, DMS shall direct the security configurations on MFN-3.
- **Common Services (CS) or similar VRF:** The CS routing domain is considered the state Agency's intranet protected by the MFN-3 Enterprise Firewall perimeter. The Common Services VRF will be connected to the Internet. At the sole discretion of DMS, DMS shall direct the security configurations on MFN-3. The Customer will be required to have a premises- based firewall with the applicable security configuration. This premises-based firewall can be Customer-owned or rented from MFN-3 with optional Vendor managed configuration.
- **Private VRF:** The Private routing domain does not inherently provide Internet access. Internet must be provided by either a separate connection to the Common Services VRF or Public VRF (OEU) or by another external ISP connection.

Based on the minimum requirements provided above in this section, provide a detailed description of the proposed service functionality to facilitate VRF structure(s) that addresses the above. This must include, but is not limited to, layout/design, standards to be used, and any other attributes designed to meet the HA/HR needs for MFN-3's communications infrastructure. For clarity, describe the ability to segregate traffic to facilitate Customer needs and promote efficient routing.

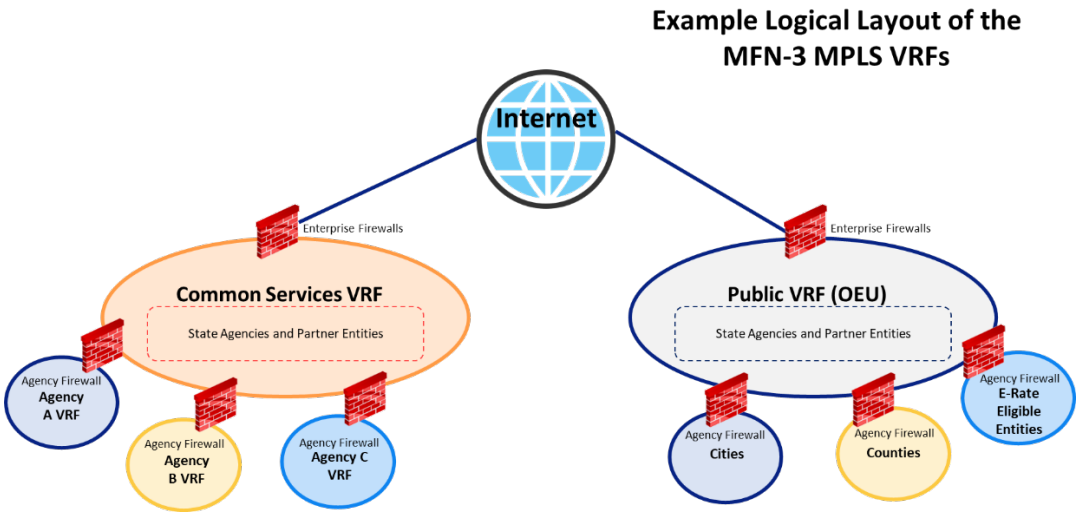


Figure 4: Logical Layout of MFN-3 MPLS VRFs

2.7.4 Management Strategy and Structure

Propose the strategy and design for providing information flows to support NMS functionality, security oversight, and tools access and how MFN-3 will be managed. Discuss all network assets including the router, a site firewall, VPN, and premises devices. This may include a discussion of the management tools; however, the focus is not the NMS, that NMS narrative is expected to be placed in the tools section.

2.7.5 Core Internet

The overall design of the statewide Internet services shall include, but is not limited to, layout and design, standards to be used, location of sites, and any other attributes designed to meet the high availability and high reliability needs of the State's communications infrastructure. For clarity, describe interconnections between components and describe the Internet infrastructure with a drawing. Subscription to a core port and local loop access is required to subscribe to Internet service. In addition, LAN to LAN VPN Service has the option to subscribe to Core Internet without a Core Port. Customers may or may not provide Internet access to their end-user clientele; access to the Internet is a Customer policy option.

Describe the overall architecture of the Internet gateway connections. Provide detailed descriptions of the Internet service that addresses the following:

- Required robust, highly available Internet gateway services.
- A proposed Internet service design that must be configured to permit gateways to back each other in case of a link failure.
- The design must utilize at least two gateways in geographically diverse cities. Define the location of each gateway.
- A proposed design for Internet access services that must not have any single point of failure between the MFN-3 Core Infrastructure and the Internet gateways.

- Provide detailed technical diagrams and related narratives on the rationale for the proposed design to assure DMS that HA/HR is fundamental to the proposed infrastructure.
- Provide a proposed design utilizing a tier 1 ISP as a transit provider for the MFN-3 Internet connectivity with the requirement of a minimum of two georedundant MFN-3 peering locations. Specifically discuss how HA/HR will be assured for the proposed design.
- Utilization of operational processes to assure HA/HR, for example, prohibiting maintenance efforts from being done on both geographically diverse gateways in the same maintenance window.
- Production testing of different failure scenarios prior to moving any sites to MFN-3.
- Customers must be able to access the Internet at the capacity of their subscribed core port speed if connected via a WAN service.
- Bi-directional forwarding (BFD) must be enabled globally across the network infrastructure. BFD must be configured for all relevant routing protocols.

Provide a detailed description of the proposed Internet service functionality via MFN-3 Core Infrastructure.

2.7.6 Enterprise Quality of Service (QoS)

MyFloridaNet-3 must be able to assure Customers that critical applications receive SLA contracted resources across the network, despite varying network traffic loads - hence the need for Enterprise QoS.

2.7.7 MPLS

Multi-Protocol Label Switching, MPLS, is to be a fundamental technology of MyFloridaNet-3.

Describe the proposed MPLS functionality.

Describe the Services provider's proficiency in implementing and operating MPLS on a large-scale Enterprise.

Describe the methods used to distribute labels. Include why this method was selected compared to other available methodologies.

Describe how the solution will support L3VPN and L2VPN services.

Describe the proposed control plane solution.

2.7.8 Multicast Functionality

Describe the proposed Multicast functionality and the manner in which the functionality will be provided.

2.7.9 MFN-3 Services Infrastructure Build-Out Plan Narrative

Provide a detailed narrative describing the MFN-3 Services Infrastructure Build-out Plan in reply to this subsection.

The Services provider must also provide project management services in accordance with the requirements of Rule 60GG-1.004, Florida Administrative Code. A Project

Management Plan and Implementation Schedule shall be submitted as a Microsoft Project document. Include sufficient detail to address all phases of the project. Include detailed timelines and activities with deliverables and milestones that will be used to track progress toward the goal of implementing MyFloridaNet-3.

Submit the Project Management Plan and Implementation Schedule in the reply packet in accordance with the instructions provided in ITN **Attachment E, Reply Format**, TAB 7.

2.7.10 Highly Available and Highly Reliable Design Characteristics

MFN-3 functionality provides support for mission critical agency Customers. The Services provider is therefore required to provide hardware, software, and processes designed to be highly available and highly reliable (HA/HR).

The design characteristics for HA/HR are as follows:

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

2.7.11 High Availability and High Reliability Strategy for the MFN-3 Core Infrastructure Services

All MyFloridaNet-3 Core Infrastructure Services and offerings must have high availability and high reliability to properly support the wide range of mission critical applications. DMS requires that its Core Infrastructure Services be provided on a carrier-class network where service characteristics including monitoring, service restoration, and capacity are considered critical. Define the strategy to be used for providing high availability and high reliability within the proposed Core Infrastructure Services. Indicate how the proposed Core Infrastructure Services support the goal of 100% uptime; an uptime of 99.99% is required. MFN-3 must provide media diversity. Identify any limitations for Core Infrastructure Services diversity.

Describe any known limitations on redundancy such as those requiring human intervention. Redundant infrastructure components are required and shall be highlighted within the proposal. Designs for all aspects of MyFloridaNet-3 and its service components must avoid any single point of failure. Ensure that bandwidth is sufficient to handle all traffic if a failover between IAGs occurs.

2.7.12 Physical Security as a component of High Availability and High Reliability

The physical security of network components (such as buildings) is of significant concern and must be defined as part of this proposal. DMS personnel will be allowed access to these facilities at any time with at least one business day's advance notice.

Provide explicit accounting for each node facility including:

- Physical address
- Leasing periods, when applicable
- Physical access, and other business considerations to permit a full understanding of security from a business perspective.

2.7.13 Power Supply as a component of High Availability and High Reliability

The Services provider is to provide backup power supply to core facilities. Backup power can be in the form of standby generators. SLAs will not be waived if the Services provider's (or any subcontracted entities') HA/HR designs are not adequate.

2.7.14 Minimal Convergence Times as a component of High Availability and High Reliability

As a component of the HA/HR strategy, DMS requires minimal convergence times, which shall be achieved through, at a minimum, the following requirements.

- Bi-directional forwarding (BFD) must be enabled globally across the network infrastructure. BFD must be configured for all relevant routing protocols.
- Fast Re-Route (FRR) must be supported for all implementations.

Describe:

- The specific design elements used to assure minimum convergence times to restore services by re-routing around component failure related to Core Infrastructure Services. IP core functionality must be designed to provide rapid core and link failure re-routing.
- The delta between a link failure and a stable state of service over the new topology.
- The expected convergence times for the proposed infrastructure.
- How the proposed Core Infrastructure Services would scale as the number of access sites/devices increase over the life of the contract.

2.8 Access Service – Statewide Wide Area Network (WAN)

This must be delivered through a <u>commercial solution</u>.

To promote competition, competitive access providers and their unique access technologies must be accommodated within the MyFloridaNet-3 Infrastructure from the MFN-3 Services provider's local loop partners. It is imperative for MFN-3 to support local loop access from providers statewide using a mix of technologies. As these and other local loop access technology options become viable, the MFN-3 Services provider must quickly incorporate them as local loop access options. WAN access bandwidth must be delivered symmetrically.

2.8.1 High Availability and High Reliability Strategy for Access and Aggregation Services

All MyFloridaNet-3 access/aggregation services and offerings that are classified as an "on-net" service must have high availability and high reliability to properly support the wide range of mission critical applications. DMS requires that its access/aggregation be provided on a carrier-class network where service characteristics including service restoration, and capacity are considered critical. Aggregation circuits to the MFN-3 Core Infrastructure are critical and must be geo-redundant. Aggregation circuits will be responsibility of the Services Provider and must be bundled within the local loop access charges in the WAN access Price Workbook entries.

Redundant infrastructure components are required and shall be highlighted within the proposal. Designs for all aspects of the connections created and established to the MFN-3 core infrastructure and its service components must avoid any single point of failure.

Define the strategy to be used for providing high availability and high reliability within your proposed access and aggregation services. Connections created and established to the MFN-3 core infrastructure must provide media diversity. Identify any limitations for access and aggregation diversity.

2.8.2 Statewide Wide Area Network (WAN) Pricing

WAN pricing is submitted on the "WAN Access (Ethernet)" sheet of the Price Workbook. Customers will use that information to make a bandwidth selection for their connectivity between the end-site and the core facility.

2.8.3 Multiple Paths Support into Core

The major causes of downtime are failures in the infrastructure between the Customer site and the MFN-3 Core Infrastructure (both the local loop, and aggregation infrastructures to the MFN-3 Core Infrastructure port). To minimize this issue for MFN-3, DMS requires the Respondent to implement an engineering design strategy where multiple paths terminate to two or more PEs with a minimum requirement of one VLAN per geographically diverse PE for all Customer connections where the primary EVC will utilize the geographically closest PE. The WAN access pricing in the price workbook must be inclusive of this minimum requirement. Preference for EVC is that the paths remain within the state of Florida boundaries. The VLANs must be geo-diverse for each Customer connection and must take separate paths from the Wire Center to the PE. Each of the VLANs for each Customer connection must not take the same path within the Access Infrastructure including the Aggregate circuit that connects into the PE. The Respondent is responsible for maintaining all bandwidth requirements related to the aggregation circuits in order to meet all service levels. The goal is to promote HA/HR by using a design strategy that provides redundant connections to core nodes.

Describe the proposed design meeting the minimum requirements above.

Describe the business and technical tradeoffs, including any unintended consequences of such a design.

2.8.4 End-To-End Integration

From the perspective of DMS and its Customers, configuration management, performance monitoring, and health monitoring must be uniform across the various partners and their technologies.

Define where any local loop access services characteristics will not appear seamless end-to-end.

2.8.5 WAN - Underlying Technology and Interconnections with Partner Infrastructures

Respondents are required to provide not to exceed pricing for the life of the contract for both access media types(fiber and coaxial). The proposed access media type(s) must meet the requirements of SLAs.

Provide descriptions that cover SLAs, Aggregation circuits to PE implementations, technologies utilized, and the like and include the following:

- A description of the basic infrastructures used for the various WAN access services.
- List the technical considerations to be used by the Respondent when selecting the technology to be used to support a Customer connection.

Include a discussion of the Respondent's interconnections to its various partners and subcontractors.

2.9 Metropolitan Area Network (MAN) Service

MFN-3's MAN connections are not connected to MFN-3 core and are therefore less expensive when compared to the WAN access transport service as it doesn't use any of the aggregation circuits. MAN service is considered an off-net service.

Sites within a MAN that have a requirement to communicate with each other can only be provisioned using a single local loop provider. MAN service includes the local loop access that is the physical link or circuit that connects from the demarcation point of the Customer premises to the edge of the carrier or telecommunications service provider's network. MAN service shall include all the necessary components such as a service provider's port to switch traffic from location to location. In addition, any necessary equipment such as termination device(s) required at the Customer premises and carriers' network shall be included as part of the service.

Considered a local transport service, MAN connections are used to group sites that have a need to communicate within their specific working group; closed-user-groups (CUG), are administrative groupings enforced by technical features within the Metro-E specification. MAN connections and CUG cannot cross LATA boundaries.

The service must provide Layer 2 connectivity support.

Describe the proposed MAN services, including regional availability and accounting for the requirements in this section.

2.10 Point to Point Transport Services

Point to Point transport services provide for direct connections between two end-sites that have requirements to communicate directly without using the MFN-3 core network. Point to Point is classified as an “off-net” service

Respondents should detail the method they are proposing to provide point to point transport services. Discuss any details of the service, including at a minimum:

- Technology type
- Network availability
- Geographic availability
- Any options for redundancy or resiliency
- Bandwidth availability
- Latency and Performance
- Customer alert notifications and incident creation, including timely updates to the MFN-3 Services Provider
- Mean time for service restoration
- Chronic event handling

2.11 Offnet Service - Cable Internet

Cable Internet is Internet access delivered via coaxial cable infrastructure, which is typically shared among users in a geographic area. Please provide information detailing your service offered, including the following criteria and any other pertinent information you would like to share about the service:

- Speed tiers (e.g., 100 Mbps, 500 Mbps, 1 Gbps)
- Symmetrical vs. asymmetrical speeds
- Support for static IP addresses
- Network management and throttling policies
- Plans for adoption and rollout of newer DOCSIS standards and associated speeds in Florida

2.12 Offnet Service - Cellular Internet

Cellular Internet is Internet access delivered via cellular mobile networks (4G LTE, 5G), typically using SIM-enabled routers or hotspots. Please provide information detailing your service offered, including the following criteria and any other pertinent information you would like to share about the service:

- Network coverage maps (urban, rural, remote areas)
- Data plans (unlimited, capped, throttled after threshold)
- Speed expectations (4G vs. 5G)
- Latency and jitter benchmarks
- Device options (hotspots, routers, embedded modules)
- Failover capabilities
- Roaming and multi-carrier support

2.13 Offnet Service - LEO (Low Earth Orbit) Satellite Internet

LEO Satellite Internet is Satellite internet provided by constellations of low-orbit satellites. Please provide information detailing your service offered, including the following criteria and any other pertinent information you would like to share about the service:

- Coverage areas
- Bandwidth and latency expectations
- Installation requirements (dish, power, line of sight)
- Weather resilience
- Data caps or fair use policies
- Portability and mobility options
- Government or emergency use prioritization

2.14 Offnet Service - DIA (Dedicated Internet Access)

DIA is Internet access with a dedicated, uncontended connection to the ISP. Please provide information detailing your service offered, including the following criteria and any other pertinent information you would like to share about the service:

- Guaranteed symmetrical speeds
- Redundancy and failover options
- Last-mile technology (e.g. Fiber, Ethernet over copper)
- 24/7 monitoring and support
- Scalability and upgrade paths
- Bundled with DDoS protection
- List any optional features available as part of the service offering such as BGP peering with a Customer provided ASN.

2.15 Other available Off-Net Transport Services

Please provide any other available off-net transport services that were not specifically listed above that you would like to offer to the State. Include any pertinent information as to how this service will be delivered and supported from both a technical and SLA standpoint. If other Offnet Services are provided, include an SLA table for each proposed service.

2.16 Daily Operational Management, Tools, and NOC

Tools in this section can be delivered either through a dedicated or commercial solution.

This section covers daily operational management, tools, and the Respondent's NOC support. The elements of this section are inherent features of all MFN-3 services and therefore there is no specific entry within **Attachment K, Cost Reply Price Workbook**. All tools required within this section are to be at a minimum in a dedicated tenancy for the exclusive use of MFN-3.

2.16.1 Day-to-day Responsibility is provided by the Services provider

Operational management is a critical component in overall quality and cost effectiveness of the statewide Enterprise. MyFloridaNet-3 daily operational management to be performed by the Services Provider includes change control, alert monitoring and data collection as well as the typical installation, turn-up, and end-site support/management. Daily operational management will be the responsibility of the MyFloridaNet-3 Services provider, not DMS. All day-to-day responsibilities are performed by the Services Provider.

2.16.2 Scope of Operational Management (Operational Support)

Operational management must support all services and technologies regardless of whether or not the CPE is Services provider-managed or Customer-managed. However, daily operational management does not include configuring CPE routers unless a Customer subscribes to a monthly configuration service option for configuration management.

Operational monitoring is considered an inherent MFN-3 function applicable to all services. Proactive monitoring for up/down status and general operational health for all sites and service components is the responsibility of the Services Provider. Daily operational monitoring shall be provided for all CPE.

All sites and service components that are part of supporting MFN-3 infrastructure must be monitored with notifications, traps, and/or alerts provided from the performance monitoring system(s).

2.16.3 Network Operations Center

Issues management is provided by the Services provider's Network Operations Center (NOC). The MFN-3 NOC shall provide remote proactive monitoring of Customer networks and systems using a centralized monitoring tool and a group of technical personnel. The MFN-3 NOC shall be in operation 24 hours a day, 7 days a week, 365 days a year, for coordination and resolution of network events. The MFN-3 NOC shall proactively monitor all aspects of the fault, configuration, accounting (network usage, user access, configuration changes, etc.) and performance.

The Services Provider is required to provide a live person MFN-3 NOC helpdesk function to be able to receive trouble calls and changes 24x7x365 for all services and components. The Services provider's NOC facilities are required to be geographically redundant and operate in a carrier class facility with backup power, and redundant systems. The redundant system for tools must be housed in the geographically redundant facility.

Define how the Respondent's standard NOC will be implemented and describe its daily operational functionality. Describe the NOC and its role as the single point of contact for any trouble isolation and resolution that addresses any trouble isolation and resolution. The Services Provider's NOC must have the responsibilities noted above, and at least the following items listed below:

- A facility located within the United States of America which is physically secured to permit entry of only authorized personnel, as determined by the Contractor.

- USI: Unique Service Identifier is used as an intelligent name for NOC monitoring. Example: MFN-DHSMV-BNNL-01. (MFN)=Vendor (DHSMV)=state agency (BNNL)=city (01)=circuit sequence.
- Accept trouble reports submitted through telephone, online portal and electronic methods from all Customers including non-credentialed Customers and authorized representatives.
- Test all services and MFN-3 Services facilities as necessary to resolve the problem.
- Proactively provide the Customer with detailed problem status updates by email, SMS, or automated telephone calls, following notification timelines and methods appropriate to the severity of the outage and the priority level of the agency, as determined by DMS.
- Allow Customers and the Department to obtain real time 24/7 problem status of service request through a web-based portal.
- Escalate troubles to higher-tier support upon the Customer's request.
- Proactively check for active alarms.
- Proactively escalate trouble tickets as necessary to the Services provider's service manager, as well as higher tier support groups.
- Cooperatively test with the Customer or authorized representative when necessary.
- Provide single point of contact function for communications with the Customer.
- Upon initial contact for a new trouble ticket, provide the trouble ticket number to the Customer or authorized representative.
- Open trouble tickets and provide logging (tracking) of the trouble ticket for issues; actions continue until a permanent resolution is implemented.
- Update and monitor trouble ticket status.
- Forward trouble tickets to appropriate groups.
- Close all trouble tickets with the agreement of the Customer or authorized representative.
- After an issue has been mitigated, in response to a request from DMS or the Customer, within five business days the Services provider's NOC will publish a Reason for Outage (RFO) in sufficient detail to allow DMS and the Services provider to take actions as lessons learned. The Services provider shall be responsible for taking all necessary steps to ascertain the RFO.
- As part of the closure process, the Services provider's NOC will assess current operating environment, controls, and configurations for all related systems including monitoring and reporting thresholds.

2.16.4 Services provider's Network Operations Center Implementation and Functionality

There will be no limitation on the number of calls or electronic requests to the Services Provider's NOC.

2.16.5 DMS Network Operations Center Oversight Responsibilities

In addition to the Services Provider's NOC, there is a DMS NOC to monitor the Services Provider's daily operations systems and processes for all technical specifications of MFN-3.

2.16.6 Maintenance Notifications and Change Control Processes

As part of the change control process, the Services Provider is required to utilize DMS's CSAB SIMS ticketing system to submit all Change Management Requests (CMRs) for DMS review and approval. This is inclusive of local loop provider maintenance activities. DMS requires a two-week advance notice for maintenance activities for the components of the MFN-3 Services Infrastructure. For those maintenance efforts, the Services Provider is required to follow the MFN-3 change control process including maintenance window(s).

Any such infrastructure changes impacting DMS Customers must be approved by DMS prior to any change by way of an electronic request. Every service impacted by the change must be identified at the time of change submittal.

The MFN-3 maintenance window shall be Sunday Evenings/Monday mornings from 10:00 PM – 4:00 AM (Eastern Time). Special maintenance windows required for DMS Customer requirements shall be at the sole discretion of DMS.

In the case of urgent maintenance, which may or may not have an emergency nature and carries enough justification to complete within a shorter term, escalation will be required to approve. Urgent maintenance events require an Emergency Change Management Request (ECMR) be submitted via the SIMS system and approved by DMS.

In the case of break-fix maintenance, which is unplanned and typically required to correct a problem of an emergency nature or to prevent large-scale impacts to the network, prior approval from DMS is not required to begin restoral activities. The Services Provider will submit an ECMR to track the changes made after the immediate impact is restored.

DMS requires an automated notification process designed to provide a list of sites potentially impacted by the change/maintenance activity. This process will be managed with the SUNCOM Incident Management System (SIMS) for automated Customer notification designed by DMS. This process can be changed at the sole discretion of DMS. Tickets opened to facilitate the change must be closed within two working days of the completion of the change.

2.16.7 Proposed Escalation Process

Provide a proposed escalation process that addresses the following:

- An escalation process initiated by the Services provider covering service outages, degraded performance, and failures of business processes.
- A clear indication of the escalation process, the tier structure, and where individuals/groups appear within the escalation process, in addition to providing DMS with an internal distribution list for escalations.
- Roles and responsibilities must include the Respondent's NOC staff, the DMS NOC staff, and the Customer staff.
- At any point, DMS or any Customer staff may request an escalation by submitting through the SUNCOM Incident Management System (SIMS), or by calling the Services Provider's NOC, the DMS NOC, or via email to either group.

- If issues are not resolved in a timely manner to DMS's complete satisfaction, the Services Provider agrees to have a corporate executive (for example, an executive vice president or C Suite representative) address such issues in a meeting; the time, date, and location determined by DMS.
- The titles of those in the corporate structure, along with a description of their involvement in the escalation process.
- Clear description of how escalated tickets will be entered into the electronic app/medium/portal selected by DMS.

2.16.8 Effective Operational Management within Logical Partitions

A fundamental requirement of MFN-3's operational management is the ability to establish logical partitions of the Enterprise facility that will be defined as dedicated networks for specific Customers or VRFs.

Discuss how the proposed operational management tools and services are effective within an overall network and within each of the logical partitions.

2.16.9 Network Management System (NMS) and Security Tools Access

DMS requires single sign-on for all tool components.

There must be no limitation on the number of licenses to access the NMS tools and security suite.

Each sign-on access requires a unique account.

A "single pane of glass" web-based online portal shall be provided to DMS by the Services Provider for a global view into the Services Provider's services to monitor trouble tickets, enabled by the integration between the Services Provider's NOC and the DMS NOC.

2.16.10 Internet Access to Tools

The Respondent's operational services will be provided to Customer staff and DMS via web accessible interfaces using a standard web browser.

Public Internet access 24x7x365 is required.

2.16.11 Customer Segregated NMS Views

DMS will extend the Services Provider's NMS views to all Customers permitting Customers to migrate away from their current NMS tool if they desire. NMS views must permit each Customer to view their individual service domain. Customers must not be able to view other Customer domains; limitations on scope of view and scope of command are necessary.

DMS requires that Customer partitions and views are able to be customizable by the Customer, instead of a blanket globally defined view that the Customers cannot alter. Each access requires a unique account. DMS requires a global view of tools, core equipment (where dedicated), services and CPE.

Define how the NMS will accomplish these different view scenarios for the different tool suites.

2.16.12 Sharing Management Tools

DMS, Customers, and the Services provider's management staff will share management tools. DMS requires view access to the same parameters the Services provider uses to manage all MFN-3 service components. DMS requires an unlimited number of user accounts for access to the NMS and security tools.

2.16.13 Special Handling for Public Safety

Agencies and local governments dealing with public safety take precedence and will be given high priority within the Services Provider's NOC queue. This precedence will be assigned for Critical and Major Ticket classifications in the event of resource limitations due to a regional event. An event could be caused by a serious storm in an area. The Agencies and local government entities listed below have a user community identified as public safety. Additional agencies and entities will be added if required.

- PSAP – 911 Public Safety Answering Point (Local Governments)
- FDLE – Florida Department of Law Enforcement
- DHSMV / FHP – Department of Highway Safety and Motor Vehicles – Florida Highway Patrol
- FIN – Florida Interoperability Network
- DOT – Department of Transportation
- DCF – Department of Children and Families' Abuse Hotline
- DEM – Division of Emergency Management
- DMA – Department of Military Affairs
- FWC – Fish and Wildlife Conservation Commission
- DEP – Department of Environmental Protection
- Local Police Departments and Sheriff's Offices

2.16.14 Ticket Classifications Based on Problem Severity

There shall be five severity classifications within the Services Provider's NOC function: Critical, Major, Minor, Chronic, and Informational. In addition, status updates will be provided to the Customer by the Services provider's NOC staff per the "Notification and Status Commitment" table in this section.

- For Critical troubles, resolution efforts occur on a 24x7x365 basis, and status updates are provided to the Customer until the problem is resolved and service has been restored. Critical problems are defined as those affecting 10 or more sites, or within the MFN-3 core that impacts a large number of users with no immediate work-around. Situations where contracted performance SLA thresholds are exceeded are also defined as Critical. The condition includes a critical work stoppage or service degradation prohibiting access to mission critical applications. A critical condition within the MFN-3 core would consist of hardware or software failure causing a work stoppage or service degradation. If the critical trouble has a common event, a single master ticket can be opened listing all impacted sites. Critical issues require a specific "critical outage notification process" which is to be defined during development of the operations guide.
- For Major troubles, resolution efforts occur on a 24x7x365 basis, and status updates are provided to the Customer until the problem is resolved and service has been restored. Major problems are defined as those affecting an individual

site with no immediate work around. The condition includes a critical work stoppage or service degradation prohibiting access to mission critical applications during the Customer's normal working hours. Situations where contracted performance SLA thresholds are exceeded are defined as Major.

- For Minor problems, resolution efforts occur primarily during regular business hours with coordinated after-hours testing with the Customer to minimize interference with performance or downtime for the Customer during regular business hours. Minor problems are defined as affecting individual sites, and do not interrupt service, degrade performance or exceed SLA specifications.
- Informational tickets are created by the Services provider's NOC when a Customer places a phone call to report an issue that may trigger an alarm for the Services provider's NOC or to request informational assistance.
- Examples of informational problems include:
    - Customer reports the network will be down for maintenance.
    - Customer reports a scheduled power outage.
    - Customer reports equipment shutdown for office remodeling.
    - Customer request information or clarification on MFN tools or operation.
    - Informational alarms from various systems and tools.
- Chronic tickets are opened at the onset of the third occurrence of the same trouble type for a specific site within a 30-day period (a 30-day moving window). Chronic tickets are only to be used to consolidate and track repair events within the individual outage tickets. Chronic tickets shall be opened under the Major classification and noted in the problem description area as chronic.

Tickets opened under the following types will be excluded from the chronic ticket formula:

- Customer Maintenance
- Customer Education
- Customer Equipment
- Duplicate Ticket
- Weather related
- UPS issue
- Site Power

Table 2: Notification and Status Commitment Table

Notification and Status Commitment Table		
Severity Level	Notification Time	Commitment
Critical	15 minutes	Initial contact to Customer within 15 minutes of an outage. Within 1 hour Customer will be contacted with cause of outage and every 1 hour with status updates.
Major	15 minutes	Initial contact to Customer within 15 minutes of an outage. Within 2 hours Customer will be contacted with cause of outage and every 2 hours with status updates.
Minor	30 minutes	Initial contact to Customer within 30 minutes of a trouble report and updates when conditions change. Within 2 hours Customer will be contacted with cause of issue. Depending on the issue, Customer will be provided with status updates every 2 hours.
Chronic	As Appropriate	Customer will be advised of chronic status and updated as conditions change.
Informational	As Appropriate	Contractor's NOC will respond to information requests within 72 hours otherwise NOC notification is not required.

Notification or Status can be provided via email or phone within the given timeframe. Customers may also call the Services provider's NOC or access the Services provider's Ticketing System at any time to obtain current status of a ticket.

Customers or DMS may contact the Services provider's NOC to change the classification of the ticket to the next higher level. For example, from "Major" to "Critical".

Please explain how the respondent intends to meet these requirements and propose any redlines/edits to this process.

2.16.15 Ticketing System Requirements

Contractor is required to provide a trouble ticketing service for the management of tickets related to performance concerns, and the Contractor's corresponding remediation efforts. Contractor will work to resolve tickets twenty-four hours a day, 365 days of the year. At a minimum, the ticketing system must have the following:

- The trouble ticketing functionality must provide online access with DMS having a global view but restrict Customers to be able to view only their tickets.

- The ticketing system must have the ability to interface with other ticketing systems.
- DMS requires a ticketing system that generates tickets automatically.
- History logs must contain chronological activity information for restoring service for any outage.

2.16.16 Proposed Ticketing System

Provide a detailed description of the proposed ticketing system.

Define any limitations/restrictions on use by either DMS or Customer staff.

Describe the functionality for automated processes where tickets are generated for SLA violations or for conditions of interest that might not be an actual SLA violation.

Describe all the trouble ticket fields.

Describe how the Services Provider has implemented the functionality proposed in this subsection within at least one other network. If the Services Provider has not implemented the functionality in another network, explain why it is being proposed and when it will be available for implementation.

2.16.17 Proposed Logging and Archival Process

The logging and archival process can be provided by several distinct systems and does not have to be integrated into a common system.

- DMS requires a minimum of 36 months of raw logs to be archived.
- Logging must include all logs from tools, and devices.
- All logs must include a hostname of the device being logged.
- DMS requires functionality that actively logs and tracks the Remote Partner activity as these partners' access intranet resources. These activity tracking features must include a mechanism for the Services provider to monitor activity showing source and destination IP addresses for each VPN tunnel and LAN-based appliances.
- For IP flows, provide technical details related to how the logging and archival service will be implemented, and its day-to-day functionality.
- DMS requires direct access to raw, unaltered IP flow logs (IPFIX, NetFlow v9, J-flow), in order to facilitate general traffic studies and requests for various audits. To support IPv4 and IPv6 traffic monitoring, DMS requires the ability to record and store IP traffic flows (500:1 sampling). In addition to IP flows, logging must include system logs from tools and devices Enterprise Firewalls, VPN devices, and routers.

Describe the technical detail related to how the logging and archival service will be implemented, and its day-to-day functionality.

Describe how logging will be supported for all services.

Provide a detailed explanation of how backups of both current and archived information will be handled.

Describe how the Services Provider has implemented the functionality proposed in this subsection within at least one other network and indicate the size and scope of

the implementation. If the Services Provider has not implemented the functionality in another network, explain why it is being proposed and when it will be available for implementation.

Describe any additional functionality in the proposed system.

2.16.18 Proposed Traffic Analyzer

Define the functionality of the system to provide a web-based management dashboard for IP flows. The system must provide these dashboard views, and reports, across all MFN-3 applications (data, voice, and video). The solution must allow a Customer to understand how application traffic is impacting network performance.

The traffic analyzer functionality can be provided by several distinct systems and does not have to be integrated into a common system.

Describe how the Services provider has implemented the functionality proposed in this subsection within at least one other network. If the Services provider has not implemented the functionality in another network, explain why it is being proposed and when it will be available for implementation.

Describe any additional functionality in the proposed system.

2.16.19 Proposed SLA Performance Monitoring Service Functionality

Describe the following in the proposed SLA performance monitoring service and any additional capability and functionality of the proposed tool:

- The reporting and web accessible view functionality to be provided. Include all necessary information in this description of the proposed SLA performance monitoring service to provide a clear understanding of how the service functions.
- A reference to the placement of probes.
- Where dedicated, a description of how a fully meshed core configuration will be established for every backbone QoS queue.
- Information outlining any mechanism to monitor the performance monitoring system itself for possible failures. The design shall allow an accurate assessment of how the local loop and CPE are performing utilizing the best-effort queue by default. The description of the monitoring service must allow DMS to clearly determine these and other facets of the implementation.
- An explicit statement assuring that the implementation of the monitoring will not impact the performance of critical networking services supporting delay sensitive traffic and public safety. Diagrams or other descriptive strategies are encouraged.

Discuss the integration of SLA performance monitoring with other operational tools within this section.

Describe how the Services provider has implemented the functionality proposed in this subsection within at least one other network. If the Services provider has not implemented the functionality in another network, explain why it is being proposed and when it will be available for implementation.

Describe the reporting, screen view, and web accessible view functionality to be provided, and any additional capability and functionality of the proposed system.

2.16.20 Proposed Configuration Management System

The Configuration Management System must have, at a minimum, the following:

- The system must archive a minimum of 25 configuration changes.
- The system must be capable of generating a display/report comparing configuration differentials, the user-account ID that made the change, and the time the change was made.
- The system must generate e-mail notifications when a configuration change has been made to a device. Notifications must include configuration differentials for review. If included in the differential provided in the notification, secrets such as passwords or other confidential information must be redacted.
- The system must support all the various dedicated equipment types found on MFN-3.

Provide a detailed description that includes at a minimum, the following in the proposed configuration management system.

Describe how the Services provider has implemented the functionality proposed in this subsection within at least one other network and indicate the size and scope of the other network. If the Services Provider has not implemented the functionality in another network, explain why it is being proposed and when it will be available for implementation.

Describe any additional functionality in the proposed system.

2.16.21 Proposed Command Line Interface (CLI), SNMP and other Access Methods

For all dedicated devices in the MFN-3 infrastructure, DMS requires direct Command Line Interface access and SNMP read-only access to all devices to query real-time information. For proposed dedicated components, read-only access must include all management access protocols such as CLI via SSH, SNMP, GUI (HTTPS), API, FTPS, TFTP, RDP, etc. where available. For proposed commercial components, read-only access is preferred but not required. This includes access to configuration, interface statistics, router system statistics, and any other network service statistics through the CLI. Customer-managed devices may or may not provide the Services provider with this level of access.

DMS Customers must have read-only access to their devices, but access must be provided via a proxy viewing tool. Customers must see only sanitized configurations. Customers must have read-only access to core devices, but access must be provided via a proxy viewing tool.

DMS must have read-only access to core devices, but access must be provided via a proxy viewing tool. DMS requires CLI access over proxy access when available.

The Services provider is required to onboard DMS service accounts at DMS discretion. These DMS service accounts will be used to access MFN-3 Services Infrastructure equipment and CPE equipment.

Describe the proposed Access methods for MFN-3.

Describe how the Services provider has implemented the functionality proposed in this subsection within at least one other network and indicate the size and scope of the other network. If the Services provider has not implemented the functionality in another network, explain why it is being proposed and when it will be available for implementation.

2.16.22 Proposed Network Management System (NMS)

The proposed NMS must have, at a minimum, the following requirements:

- All objects in the enterprise map must be customizable but be read-only when it comes to populating or deleting objects.
- The system must alert for any down equipment or circuits via E-mail with a complete description of the issue.
- The system must alert proactively when defined thresholds are exceeded.
- The MFN NMS system tools capture the same time from the MFN Network time servers in UTC but correct for EST and automatically adjust for DST.
- Thresholds must be able to be set in advance of those thresholds which would be an SLA violation.
- NMS must be able to monitor all MFN-3 Services Infrastructure components.

Describe in detail the proposed NMS that includes the above requirements (include information on how the proposed NMS will monitor for all related SLAs in the SLA matrix)

Describe how the Services provider has implemented the functionality proposed in this subsection within at least one other network and indicate the size and scope of the other network. If the Services Provider has not implemented the functionality in another network, explain why it is being proposed and when it will be available for implementation and when it will be available for implementation.

Describe any additional functionality in the proposed system.

2.16.23 Proposed Performance Tools

Describe in detail the proposed performance tools to address the following. Provide a description of the proposed baseline including storage, processing power, and generally expected query response times. Provide a description of the proposed tool's default rollup process. Include a description of the parameters DMS can modify to go beyond the baseline.

- Must show graphs for each object being monitored. Must have five (5) minute, hourly, daily, weekly, and yearly graphing options.
- Network and application objects to be graphed must include (at least) CPU, bandwidth, memory, latency, jitter, QoS queues, physical interface errors, server disk space, application response, and other critical events.
- Systems must be capable of monitoring all services and components under MFN-3
- Performance tools must show historical hop-by-hop latency, jitter, and graphical trace route reports.
- DMS requires the option to add data storage capacity and processing power beyond the baseline for the proposed system.

- Reporting must be able to show performance for all QoS types.
- Reports should be compiled for any time period.
- DMS and Customers must be able to generate their own reports on an ad hoc basis and as part of a predefined automatically generated reporting set.
- Tools must report on SLAs based on network performance. SLA reports must show graphs and history plus report for all thresholds exceeded.

Describe how the Services Provider has implemented the functionality proposed in this subsection within at least one other network and indicate the size and scope of the other network. If the Services Provider has not implemented the functionality in another network, explain why it is being proposed and when it will be available for implementation.

2.16.24 Current Tools

This list includes all current MFN-2 tools. This is for informational purposes and is not a requirement for MFN-3.

Spectrum:

- Network management
- Configuration management
- Performance SLA tracking and alarming

NetFlow Analysis (NFA):

- Traffic analysis
- Diagnostics
- Reporting

Performance Center:

- Performance statistics
- Diagnostics
- Reporting

Splunk:

- Performance SLA visualization

Looking Glass:

- Command Line Interface (CLI) access to routers

ownCloud:

- Document library

2.17 Customer Premises Equipment – General

The services provided in this section by the Services Provider may not be subcontracted and must be directly provided by the Services Provider. The Services Provider shall own and maintain any CPE provided under MFN-3. CPE shall include equipment such as routers, firewalls, and SD-WAN appliances.

2.17.1 Acquisition and Support Specifications for Customer Premises Equipment Supported Under MFN-3

The MFN-3 Services Provider, at the request of a Customer, must provide Customer premise equipment and related CPE configuration management for all MFN-3 services.

Configuration management is an optional service; Customers are not required to subscribe to the Services provider-managed configuration service for any MFN-3 service.

Customers can subscribe to configuration management for Customer-owned or rent CPE.

Customer provided equipment is permitted as long as it is on the Services Provider's Certified CPE List.

Customers may, but are not required to, rent equipment under this contract. Customers may rent more than one device at a site. Customers may subscribe to multiples of configuration management services for the site-specific, redundant, or spare devices.

As further described in Section 2.17.10 below, the CPE Rental Rate formula and the formula values submitted for each formula variable listed in **Attachment K, Cost Reply Price Workbook** (CPE Tabs) will be used as the basis for calculating rental pricing for all current and future equipment configurations for the life of the contract. Any modules/ports/pluggables shall not incur an installation charge in the CPE formula. Exceptions will be made to accommodate rate reductions.

Licenses shall be part of the Hardware/Software Discount in the CPE formula.

Rental CPE follows USF funding guidelines and is not available to be converted to rent-to-own.

All MFN-3 CPE shall include CPE maintenance as part of the rental pricing. Maintenance shall include but is not limited to replacement of hardware/defected part(s) and dispatches at no additional cost. It shall also include software upgrades and patches as well as upgrades to address any vulnerabilities. CPE maintenance is required that meets all applicable performance and remediation service levels.

All MFN-3 CPE is to be staged, configured, delivered, installed, rack mounted (includes the rack mounts) and turned-up on-site as part of the CPE rental pricing with no additional costs for these services. The price must be inclusive of any recurring service fees.

Standalone Customer equipment and standalone equipment maintenance are not available for purchase under MFN-3.

2.17.2 Authentication, Authorization, and Accounting (AAA)

<u>This can be delivered either through a dedicated or commercial solution</u>.

The Services provider will be required to provide AAA (access control) to Services provider-managed equipment at no charge (RADIUS, TACACS, etc.). Customers

managing their own CPE are responsible for their own access control. ~~However, Customer-managed CPE has the option to use Contractors' AAA devices and process.~~

2.17.3 Certified Customer Premises Equipment (CPE) List

To address changes to equipment availability, DMS uses the concept of a Certified CPE List to list/define specific devices approved for Customer use. The Certified CPE List is a list of equipment that has been certified by DMS and the Services Provider for use on the network. As equipment is released for sale by equipment manufacturers it becomes a candidate for inclusion in the equipment list supported by the Services Provider, but it does need to pass DMS' and the Services Provider's certification process for testing and field availability. Standard equipment will be refreshed with new hardware/software throughout the life of the MFN-3 service using the Certified CPE List strategy.

Changes to equipment and availability are expected throughout the life of the Contract, therefore the Services Provider and DMS shall discuss ad-hoc Certified CPE List updates as part of the monthly operational meetings. These changes will be proactively updated prior to Customer demand.

If equipment is not on the Certified CPE List and it is requested as part of a DMS work order, the Services Provider will immediately work to have it placed on the Certified CPE List within 60 days. If a configuration change cannot be accomplished because that feature has not been tested/certified, the Services Provider will immediately work to have the Certified CPE List updated.

Equipment provided in Attachment K, Cost Reply (Price Workbook) is considered a sample and does not represent the entire list of current CPE. Just prior to migrating the first site to the new core, DMS and the Services provider will update the equipment Certified CPE List.

As needed, DMS will review the Services Provider's Certified CPE List update process during the standing operational meetings to ensure it is effective for DMS. It is important the Services Provider establish a certification process to be effective for their operational needs. DMS wants to avoid potential delays when filling Customer orders. Therefore, the Services Provider must test or certify new equipment proactively rather than reactively, by testing new equipment quickly when released from the manufacturer, rather than reacting once an actual order has been submitted into the CSAB system.

2.17.4 Certified CPE List Process

The process below defines the general steps to be used when new equipment models are to be added to the Certified CPE List. There is to be a final Certified CPE List review prior to the MFN-3 Core Infrastructure turn-up, but DMS anticipates adopting the Services Provider's standard equipment packages. The specific Certified CPE List change process will be updated in the standing monthly operational meetings. The Certified CPE List process applies when Customers have special requirements for equipment functionality. The Services Provider will work with DMS and its Customer base using a process similar to the one outlined below for the development and implementation of equipment functionality.

- Participate in discovery/design meetings with DMS and the Customer to understand the need for a particular option or feature.
- The Services Provider and DMS Engineering teams review the requirements.
- DMS will be provided with the testing plans, and if requested, DMS can participate in these tests.
- The hardware, software, or features are tested in the Lab. Testing takes place in a reasonable length of time; no more than 60 days total unless an alternate timeframe has been previously approved by the Department.
- Upon test completion, DMS will be provided with the test results.
- When the process is complete, the Services Provider shall notify DMS that the Services Provider is prepared to support the new equipment.

2.17.5 Bi-directional Forwarding Detection (BFD)

All services shall be implemented with Bi-directional Forwarding Detection (BFD). Any site-specific exceptions will be approved by DMS.

2.17.6 Operational Parameters Related to Customer-Managed CPE Configuration

The Respondent must provide equipment at the Customer's premises and all related configuration management. However, the Services Provider will permit Customer-managed CPE as access devices for MFN-3. The Customer will have access to the proper configuration guidelines and any necessary site-specific technical data/information to support site turn-up. For troubleshooting and maintenance purposes, DMS permits Customers opting to manage their CPE the ability to enable operational management (NMS tool access) to their CPE; allowing the Services provider's NOC read/only access. Customers must be provided with appropriate access to archived configurations via the MFN-3 Portal.

2.17.7 Services Provider-Managed Configuration Management

Services Provider-managed Customers are not required to provide complete and accurate syntax when requesting configuration changes.

DMS requires the option to offer Services Provider-managed CPE where configuration changes are not performed by Customers; a turnkey solution. For the general Customer, once CPE is configured and installed, there is little effort expended to make operational updates. Therefore, DMS requires unlimited configuration changes for those sites subscribing to MFN-3's Services Provider-managed option. All services under the Site Inventory fall under configuration management.

Any features supported by the CPE manufacturer shall be enabled as part of the rate provided in the CPE Configuration Management cells on tab 9 – Ancillary Network Services in the **Attachment K, Cost Reply Price Workbook** for CPE Router, Firewall and SD-WAN Appliance. DMS requires the Services Provider to offer a full suite of hardware, software and engineering services to DMS and its diverse Customer base (including public safety). While most MFN-2 configurations are satisfied by standard templates, other configurations do exist.

2.17.8 Virtual Routing and Forwarding (VRF)-Enabled CPE and VRF-Lite Configuration Support

This CPE configuration feature is used to eliminate the need to install a second circuit (and associated CPE) when a site must support two or more routing domains on a single CPE router. A CPE running VRF-Lite is configured for two or more VRFs. The sum of the bandwidth assignments may not exceed the speed of the connection.

2.17.9 Customer Premises Equipment Response Requirements

The Services Provider is expected to provide standardized CPE offerings for Customers. In addition to addressing CPE equipment in the cost reply workbook, discuss the proposed CPE devices as follows.

Describe in detail the functionality of the proposed CPE devices, including routers, firewalls, and SD-WAN devices.

Contrast and compare the features related to why the manufacturer's CPE devices proposed has been chosen over a competing product.

Discuss how the selected CPE devices will meet the requirements described in section 2.17.

2.17.10 Customer Premises Equipment Rental Option and Price Protection

The Services Provider grants each Customer the right to rent the CPE set forth in the CPE roadmap, including all CPE listed in Attachment K, Cost Reply (Price Workbook), at any time during the initial term and any renewal term of the Contract. This option may be exercised at Customer's sole discretion, in whole or in part, and the Services Provider shall not impose any cap, minimum quantity, timing restriction, availability limitation, or other condition that would impair Customer's ability to exercise the rental option at any time during the initial term and any renewal term of the Contract.

All prices, charges, MSRPs, MRCs, and fees listed in the CPE roadmap**,** including all prices, charges MSRPs, MRCs, and fees listed in Attachment K, Cost Reply (Price Workbook), are non-escalating for the initial term and any renewal term of the Contract. In the event that the actual market MSRP (whether applicable to Hardware/Software Cost, List Price for 1 Year of Maintenance, or both) or the Services Provider's procurement cost for the CPE increases after the effective date of the Contract, the Services Provider shall continue to provide the CPE to the Customer at the MRC established in the CPE roadmap, including Attachment K, Cost Reply (Price Workbook). Additionally, all discounts listed in the CPE roadmap, including all discounts listed in Attachment K, Cost Reply (Price Workbook), may not be decreased at any time during the initial term and any renewal term of the Contract.

For any CPE not listed in Attachment K, Cost Reply (Price Workbook), that is added to the CPE roadmap after the effective date of the Contract (hereinafter referred to as "Subsequent CPE"), the same CPE rental formula (i.e., MRC) and formula values (i.e., Hardware/Software Discount; Maintenance Discount; Hardware/Software & Installation Divisor; and Installation) as set forth in Attachment K, Cost Reply (Price Workbook), will apply to such Subsequent CPE for the initial term and any renewal

term of the Contract. The Hardware/Software Cost MSRP and the List Price for 1 Year of Maintenance MSRP will remain capped as of the date the Subsequent CPE is added to the CPE roadmap in an amount that is equal to or less than the actual market MSRP as of such date. As stated in the paragraph above, the MSRP that is listed on the CPE roadmap will be non-escalating for the initial term and any renewal term of the Contract.

The Services Provider shall be solely responsible for funding any "shortfall" or difference between the fixed MSRP established in the roadmap, including Attachment K, Cost Reply (Price Workbook), and the actual market MSRP.

If the actual market MSRP decreases below the fixed MSRP established in the CPE roadmap, including Attachment K, Cost Reply (Price Workbook), the MRC paid by the Customer will remain capped at the fixed MRC established in the CPE roadmap, including Attachment K, Cost Reply (Price Workbook).

If any CPE listed in the CPE roadmap, including Attachment K, Cost Reply (Price Workbook), becomes unavailable the Services Provider shall provide a successor model of equal or superior technical specification. The rental price (MRC) paid by a Customer for such successor model will remain capped at the fixed rental price (MRC) established for the original model listed in the CPE roadmap, including Attachment K, Cost Reply (Price Workbook), regardless of any higher MSRP associated with the newer technology.

2.17.11 Return and Removal of CPE:

The Services Provider shall promptly remove and retrieve all CPE owned by the Services Provider within 20 business days following the effective date of termination or expiration of the Contract. The Services Provider shall coordinate with the Customer to schedule pickup of the CPE at a mutually convenient time and shall leave the Customer 's premises in the same condition as prior to installation, excluding (i) reasonable wear and tear and (ii) changes or damage to the Customer's premises not caused by or attributable to the Services Provider. If the Services Provider fails to retrieve the CPE within the specified timeframe, the Customer may, at the Customer's option, (i) require the Services Provider to reimburse reasonable storage fees beginning on the 21st business day, or (ii) deem the CPE abandoned and dispose of it without liability upon written notice to the Services Provider.

2.18 Remote Access -- Centralized Virtual Private Network

2.18.1 Centralized VPN Service for MFN-3 Remote Access

This can be delivered either through a <u>dedicated or commercial solution</u>.

MFN-3 requires a Centralized VPN service allowing remote sites, remote partner LANs, and remote users to access MFN-3 via a secure, encrypted VPN tunnel.

These specifications do not necessarily list all equipment or software required to produce an operational encrypted VPN Service. The Reply must contain a complete service solution with all necessary components. The Services Provider will be responsible for verifying if all components are compatible when integrated with MFN-3 and Customer systems.

The MFN-3 Centralized VPN Service must utilize strong authentication and encryption for IP data streams. In your response, please include how you will secure the solution, including details regarding encryption standards (key length, secure hash algorithm, key exchange, authentication keys, etc.) as to meet the minimum requirements listed in section 2.20.7.

Remote access for single Customer sites, or partner networks, must be governed by strong access control mechanisms, such as access policies or Access Control Lists. Access control mechanisms will cover both host applications and data sources (servers) residing behind the Internet facing MFN-3 firewall cluster. The Centralized VPN Service must provide secure connections utilizing strong encryption for all traffic traversing any path from the encrypted tunnel origination point to its termination point at the outside interface of the VPN gateway.

The Centralized VPN Service must support these designs:

- Remote site to Centralized VPN Gateway (LAN-to-LAN VPN)
- Layer-3 Client Remote User to Centralized VPN Gateway (Client-to-LAN VPN)

The following design elements are required:

- LAN-to-LAN tunnels must be VTI based with tunnels built to geo-diverse VPN gateways. BGP over the tunnels will handle failover between gateways.
- The remote user access control mechanisms (access policies or ACLs) must be configurable and enforce restrictions on access to the specific network, subnet, or single host server to the TCP/UDP port level, as required.
- The solution must provide application-based filtering and threat prevention.
- The VPN solution must support bi-directional sessions either initiated by the remote site to the Services Provider's centralized gateway or initiated by an MFN-3 site to the remote partner's VPN appliance.
- The VPN solution must map each remote partner's traffic into the appropriate VRF and cannot separate Customer s with policy based routing.
- VRF mapping is the responsibility of the Services provider.
- The VPN service must support desktops, laptops, and tablets produced by various manufactures both now and in the future which may require upgrades to the service features. The service must be compatible with the Windows, Apple, and Linux operating systems.
- Components such as hardware, software, IP transport, access port(s), VRF mapping, core access, authentication system, tracking, logging, and NOC support are bundled (inherent) in the cost elements provided in the Price Workbook.

2.18.2 Remote Site to Centralized VPN Gateway (LAN-to-LAN VPN)

This can be delivered either through a <u>dedicated or commercial solution</u>.

The LAN-to-LAN VPN implementation sends encrypted traffic from remote partner sites to MFN-3 using the Internet instead of using a direct MFN-3 wireline connection. The VPN service must provide bi-directional initiated encrypted IP connectivity for remote partners. At the MFN-3 tunnel termination point at the MFN-3 Internet nodes, the encrypted traffic is unencrypted then logically mapped into the appropriate VRF.

Traffic must be encrypted from the remote partner's premises VPN appliance to the outside interface of the MFN-3 Centralized VPN gateway. The proposed design must protect against Internet attacks and provide a secure encrypted tunnel between the MFN-3 Customer and the remote partner on the Internet. Access into MFN-3 by the remote partner must be governed by MFN-3 access control mechanisms. The Services provider will, in concert with DMS, implement policies that define the specific agency networks, subnets, or host server(s) the remote partner can access. The Services Provider is required to dynamically advertise an appropriate IP route allowing encrypted tunnels to be initiated by an MFN-3 Customer, to establish connectivity to the remote partner VPN appliance. The remote partner may utilize their own VPN appliance, or use the Services Provider provided appliance.

- **Services Provider-Provided VPN Appliance:** If the Services Provider provides the appliance, they shall install the device at the remote partner's location and assume end-to-end responsibility for elements of the service including the hardware appliance, installation, maintenance, and software configuration. The Services Provider is responsible for deploying VPN devices throughout the continental United States at no cost other than those listed in Attachment K, Cost Reply (Price Workbook). Based on the CPE type selected, there will be a CPE configuration management fee for the Vendor managing the device, as listed in the Price workbook. The CPE formula will be used to rent the CPE. There shall be no other fees such as travel or lodging. The Services Provider may subcontract with a third party company to provide the installation, or at the Customer 's request, send the hardware appliance to the remote partner preconfigured.
- **Remote Partner Provided VPN Appliance:** The remote partner may use their hardware encryption appliance as long as the appliance conforms to the MFN-3 encryption parameters and machine authentication specifications. The Services provider must configure the Centralized VPN Gateway as specified in the MFN-3Customer 's work order and provide the remote partner with all relevant programmable parameters including the applicable access policy or ACL, as required. The remote partner is responsible for their hardware appliances, including the software configurations.

Include a design narrative with diagrams as needed that describes the proposed plan to address the requirements of the subsection. Discuss the proposed plans to accomplish the requirements for in state and out-of-state installations.

Enter the appropriate costs in Attachment K, Cost Reply (Price Workbook), Centralized VPN, LAN-to-LAN.

2.18.3 Redundancy for the Centralized VPN System Components

The Services Provider must implement redundant systems in a minimum of two MFN-3 IAG complexes. Each location must include equipment to provide encrypted LAN-to-LAN, Client-to-LAN and the associated authentication and activity logging/tracking servers. This functionality may be accomplished using multiple hardware elements integrated together to function as a unified Centralized VPN System at each location. The primary and failover systems must be linked in real-time to maintain configuration and auto failover state. The failover system must (at all times) be configured with a

mirror image of the active unit(s) running configuration complete with all remote user access policies and account information.

The primary VPN system must auto-failover to the secondary geo-diverse system via BFD in less than 200ms. A failure is defined as any event that degrades IP throughput connectivity and/or the remote user's ability to login, establish an encrypted session to the VPN system solution, or the ability of the system to log or track user activity.

Include a design narrative with diagrams as needed that describe the proposed plan to meet the requirements of the subsection, including how the ancillary servers (all encryption appliances, authentication, logging, and tracking servers) will be integrated within the proposed VPN service.

Redundant design is an inherent feature of MFN-3 so there is no specific entry within the Attachment K, Cost Reply (Price Workbook).

2.18.4 Remote User Access Control Mechanisms

The Services Provider is required to configure unique access control mechanisms for each remote user (or remote user-groups) connection based on the information contained in the work order. An access control mechanism, such as access policy or ACL, must be configured on all ingress hardware or on another security appliance prior to entering the MFN-3 Core Services Infrastructure. The mechanism must incorporate programmable access features that control access to a network, subnet, or host server to the TCP/UDP port level including application-level threat filtering.

2.18.5 Network Address Translation (NAT)

The Services Provider shall not route non-approved IP address space on the State intranet. The source (Layer-3) IP address shall have the option to support NAT into an IP address range specified by DMS. NAT overload is permitted to reduce the required number of IP addresses assigned by DMS. At the Services Provider's discretion, additional hardware may be used to perform the NAT functions if required.

Describe the methodology to be used so advertised NAT-ed IP address space will take the appropriate return route to the VPN solution.

Include a design narrative with diagrams as needed that describe the proposed plan to meet the requirements of the subsection.

Network Address Translation is an inherent feature of MFN-3 so there is no specific entry within Attachment K, Cost Reply (Price Workbook).

2.18.6 Installation, Monitoring, and Trouble Reporting for LAN-to-LAN VPN

The Services Provider shall coordinate with the remote partner to facilitate and successfully establish connectivity via an encrypted tunnel. The Services Provider must monitor each LAN-to-LAN VPN connection. The Services Provider must make every effort to work in conjunction with the remote partner to resolve any outages.

As needed, the Services Provider is required to coordinate a conference call with DMS, and the MFN-3 Customer, and the remote partner to turn-up and test the VPN tunnel IP connectivity. DMS will act as an escalation point for any problems that may arise if the Services Provider encounters any cooperation issues.

The Services Provider is required to immediately notify the DMS NOC and the remote partner when the VPN tunnel goes down or is not functioning correctly. The Services Provider's NOC is required to open a trouble-ticket to document the LAN-to-LAN issue and take necessary corrective actions.

Installation, monitoring, and trouble reporting are inherent features of MFN-3 so there is no specific entry within Attachment K, Cost Reply (Price Workbook).

Provide a description of the monitoring process if the standard MFN-3 tools suite cannot be used.

Describe any limitations to using the MFN-3 tools suite in this application. In addition, describe the proposed trouble-reporting process.

2.18.7 IKE, IPSec Security Association (SA) and SSL Attribute Matrix

The following table outlines the minimum encryption requirements to be used for LAN-to-LAN VPN tunnels:

Table 3: IKE, IPSec Security Association (SA) and SSL Attribute Matrix

Encryption Algorithm	AES 256 or higher (GCM preferred)
Authentication	Certificates or passwords
Internet Key Exchange	IKE or IKEv2 (preferred)
Diffie-Hellman (D-H) Groups	Group 5 or higher
Perfect Forward Secrecy	Group 5 or higher
Data Integrity Hash Algorithm	SHA256 or higher
Pre-Shared Keys (if used)	16 characters minimum
Security Association (SA) Time	Varies per implementation
Authentication Type	Certificates or passwords
Security Association (SA) Lifetime	Varies per implementation

If the remote partner owns their appliance and it does not support D-H group 5, then D-H group 2 may be used upon DMS approval. If a pre-shared key is proposed for the LAN-to-LAN encryption appliance authentication method, the key must have a minimum character length of sixteen (16). The key must include upper/lower case, numerals, and three of the sixteen characters must be special characters such as !@#$%^&*().

Include a design narrative with diagrams as needed that describes the proposed plan to address the requirements of the subsection.

Provide a table similar to the one above indicating the encryption parameters to be used in the VPN service.

2.18.8 Client to LAN Remote User to Centralized VPN Gateway (Client-to-LAN VPN)

The Client-to-LAN service must function at Layer-3 as a traditional IPSec Client-based VPN and terminate on geo-diverse head ends. The client must be capable of automatically failing over between geo-diverse systems. HA pairs are not permitted to be built across geo-diverse locations. The client must receive a pushed IP address, become a node on the MFN-3, and function as if the remote computer resided on the internal LAN network for the Customer issuing the work order. The VPN appliance must not proxy IP packets from the remote computer; the IP packet must traverse the VPN appliance to get into the MFN-3 intranet. The encrypted tunnel terminates at the MFN-3 Internet Access Gateway node where the remote user's IP traffic is unencrypted then logically mapped into the appropriate MFN-3 VRF for the sponsoring Customer's network.

The VPN Service solution must provide connectivity for remote users connected to the Internet. For remote users, the Layer-3 Client-to-LAN VPN implementation must provide the remote user the ability to connect to the MFN-3 through a secure tunnel. The tunnel must be built from the client computer to the outside interface of the geo-diverse Centralized VPN gateway.

The Services Provider is required to configure the Centralized VPN Gateway to utilize an access control mechanism as specified by the MFN-3 Customer's work order. Before a remote device can establish an encrypted session, the remote user must successfully authenticate through multi-factor authentication.

Include a design narrative with diagrams as needed that describes the proposed plan that addresses the requirements of the subsection.

Enter the per user costs in the Price Workbook, Centralized VPN, Client-to-LAN.

2.18.9 Client-to-LAN VPN Split-Tunneling and Security Policy Compliance

The Services provider must offer split-tunneling as an option which the MFN-3 Customer can select on the work order. Split-tunneling permits remote user access to general Internet websites while at the same time being actively connected to the MFN-3. Unless split-tunneling is enabled, all IP traffic (to/from) the remote device is forced over the encrypted tunnel to the Centralized VPN gateway, where it drops all traffic not destined for resources on the MFN-3.

Before a remote device can establish an encrypted session with the Centralized VPN gateway and gain access to MFN-3, the VPN service must verify the remote device has:

- an active firewall
- up-to-date antivirus software
- up-to-date operating system software patches.

The service must actively monitor the remote computer's firewall setting, and if the firewall becomes disabled during the active VPN session the service must notify the end-user of the firewall-disabled state and terminate the VPN session. (DMS and the

Services provider will jointly define what will be considered as up to date during the MFN-3 Services Infrastructure build-out phase and update the Operations Guide.)

Include a design narrative with diagrams as needed that describes the proposed plan that addresses the requirements of the subsection.

Enter the split-tunnel cost in Attachment K, Cost Reply (Price Workbook), Centralized VPN, Split-tunnel Per-User Cost.

Installation, monitoring, and trouble reporting are inherent features of MFN-3 so there is no specific entry within Attachment K, Cost Reply (Price Workbook).

2.18.10 Multi-Factor Authentication Requirement

The VPN service must include a multi-factor login authentication method for all remote users. The authentication method must include a login username and password, and MFA. Under the multi-factor authentication process, the remote user must be required to pass both factors before a session is established with the VPN Gateway. Acceptable MFA methods do not include the use of certificates or SMS.

All necessary authentication server hardware required to build the integrated authentication system must be owned and maintained by the Services Provider in addition to being integrated with the VPN Gateway. If the reply proposes an electronic token or other type solution requiring physical distribution to the remote user, the reply must include a token distribution plan.

Include a design narrative with diagrams as needed that describes the proposed plan that addresses the requirements of the subsection.

Multi-factor authentication is an inherent feature of the VPN service so there is no specific entry within Attachment K, Cost Reply (Price Workbook).

The multi-factor authentication method must include features, which protect against malicious interception of authentication credentials.

2.18.11 Username/Password Policy Enforcement

The Client-to-LAN VPN solution must provide username and password policy enforcement, and password management. Each remote user account must have a unique username and password. The username and password must have a minimum length of eight (8) alphanumeric and special characters containing at a minimum, two (2) letters with at least one capitalized, two (2) numerals separated within the string, and one (1) special character (examples, !@#$%^&*|}{?). The system must force the remote user to change their password every ninety (90) calendar days via a self-service portal.

The VPN Service must protect against simultaneous login and shared authentication credentials by the remote user. The Services Provider is required to:

- Monitor user logon activity to the VPN appliance and log any malicious activity including any simultaneous logon attempts made by a remote user's login credentials (sharing accounts).

- Provide notification to DMS of all simultaneous login attempts. The notification must include the user account information and the captured logging record related to the event.
- At the direction of DMS, immediately suspend, disable, or delete the remote user's account.
- Have the ability to reinstate any disabled or suspended account within two (2) hours.

2.18.12 Inactivity and Duration Timeouts for Client to LAN Sessions

The VPN solution must have a programmable inactivity timer configured to drop the VPN session after twenty (20) minutes of inactivity. The VPN appliance must be configured to terminate all sessions after eight (8) hours or unless otherwise directed by DMS.

2.18.13 In Case of Emergency (ICE) VPN Accounts

The intent of "In Case of Emergency (ICE)" accounts is to provide emergency VPN connectivity to MFN-3 from sites on the Internet. The deployment process must be rapid; therefore, these emergency accounts must be pre-provisioned. (The specific processes will be defined in the Operations Guide.) Workers displaced due to circumstances such as natural catastrophe, pandemic, or any other event that prevents personnel from reporting to their workplace must have the option to use ICE VPN accounts. Based on the orders for those subscribing to this service, the authentication systems must be pre-populated with the end-user account information and related security policies. For ICE accounts, DMS will permit username and password authentication for forty-five (45) days, after which, each activated account must be reconfigured, within 30 days, and conform to the standard multi-factor authentication.

The MRC for each dormant account is considered a resource reservation fee covering hardware, licensing, and system support. The MRC covers the first 45 days of actual use. On the 46th day of use, the MRC converts to the standard VPN MRC.

Enter the appropriate costs in Attachment K, Cost Reply (Price Workbook), Centralized VPN, and In Case of Emergency Services.

2.18.14 Test VPNs for DMS

Except for the DMS VPN test accounts, VPN orders and changes follow the standard ordering and operational processes established for other MFN-3 services. At no cost, the Respondent must provide twenty (20) test VPNs. The VPNs may be used by any Customer at the discretion of DMS for test purposes. The breakdown is listed below:

- LAN-to-LAN encrypted tunnels -- five (5)
- Client-to-LAN -- fifteen (15)

Test VPNs are an inherent feature of MFN-3 so there is no specific entry within Attachment K, Cost Reply (Price Workbook).

2.18.15 End-to-end Integration Responsibility

There are numerous components to be integrated together as part of the VPN service. As an end-to-end service, the Services provider is responsible for the installation, day-

to-day troubleshooting, issues resolution, and administration of all related components. The Services Provider is required to coordinate all activities associated with related equipment installations, including coordinating inside wiring installation as required.

2.18.16 VPN Customer Migration

The number of Customers that will require LAN-to-LAN and Client-to-LAN migration is subject to change; however, a list of accounts will be provided for LAN-to-LAN and the total number of Client-to-LAN accounts. The migration shall be at no cost to DMS and the Customer. The migration plan includes:

- A seamless transfer of MFN-2 VPN subscriber accounts to the new VPN Service.
- The number of dedicated staff (both administrative and technical) that will be allocated to the migration effort.
- A comprehensive narrative, which describes how the Customer migration will be accomplished. Include a schedule and communication plan covering coordination with Customers and stakeholders.
- A test procedure that will be used to validate migrated connections.
- There is no specific reply to this subsection. The VPN migration specifics are to be included in the reply to subsection 5.1.

2.19 VPN to MFN-3

This can be delivered either through a <u>dedicated or commercial solution</u>.

While MFN-3's Wide Area Network service has wireline connectivity to the MFN-3 core via aggregate connections, VPN to MFN-3 uses the Internet to access the MFN-3 Core Network. VPN to MFN-3 can be used as a site's primary access, or as a backup connection. The following technologies shall be offered as access options.

- Cable Internet
- Cellular Internet
- DIA
- LEO Internet

All VPN to MFN-3 service options integrated into the MFN-3 core require an encrypted tunnel terminating on the Contractor-managed centralized VPN solution. Pricing for the encrypted VPN tunnel using the "Respondent Partner Provided Endpoint - First set of tunnels (including both primary and secondary)" cell in the Centralized VPN tab shall be used to connect and access MFN-3 core.

The CPE device shall have the ability to secure all information i.e. encrypt all transmitted IP traffic and by default, route the encrypted IP traffic to the MFN-3 centralized VPN solution. The Customer site will not have the ability to split-tunnel to Internet sites; all IP traffic from the Customer site must be routed to the centralized VPN solution managed by the Contractor. Customers are required to rent the CPE (with encryption capabilities) using the CPE formula and CPE configuration management in the CPE Price Sheets.

VPN to MFN-3 connectivity requirements into the MFN-3 core:

- Encrypted LAN-to-LAN tunnels must be VTI based with tunnels built to geo-diverse VPN gateways. BGP over the tunnels will handle failover between gateways.
- The VPN solution must map each remote partner's traffic into the appropriate VRF and cannot separate Customers with policy-based routing.
- VRF mapping is the responsibility of the Services Provider.
- Bi-directional forwarding (BFD) must be enabled globally across the network infrastructure. BFD must be configured for all relevant routing protocols.
- The VPN requirements specified in the table under Section 2.20.8 shall apply.

Describe the proposed VPN to MFN-3 solution and include a diagram of the VPN to MFN-3 service components as proposed.

2.19.1 VPN to MFN-3 Monitoring and Operational Management

Describe the proposed monitoring functionality considering the following criteria. Respondents are encouraged to provide monitoring beyond the minimum requirements listed below; however, the goal of this service is an overall low cost solution.

- NetFlow-based reports must be provided within the standard suite of NMS reports.
- Traffic flow analysis or the SIEM tool will receive NetFlow from the MFN-3 core infrastructure for all connections.
- At a minimum, Ping for up/down status is required for VPN to MFN-3 monitoring functionality.
- The Services Provider must support SNMP for VPN to MFN-3 sites if they enable SNMP.
- MFN-3 operational monitoring system will send an email alert to the VPN to MFN-3 site contact for up / down monitoring.
- Similar to the operation support provided under WAN, the Services Provider's NOC is responsible for VPN to MFN-3 for trouble reporting and resolution; Customers must not see any difference in the two services.
- VPN to MFN-3 site status is part of Enterprise level view. DMS and the Customer will see VPN to MFN-3 sites as part of the NMS tools suite

2.20 SD-WAN Software Defined Wide Area Network

This can be delivered either through a <u>dedicated or commercial solution</u>.

A comprehensive hosted Software-Defined Wide Area Network (SD-WAN) solution must be provided. The goal is to enhance network performance, security, and scalability across various state government departments and remote locations.

As part of this procurement, a "turnkey" hosted Software-Defined Wide Area Network (SD-WAN) solution will be made available. As a turnkey solution, there are no other components to be supplied by DMS or the Customer. **All system software/hardware necessary to support the SD-WAN Service must be provided and included in Attachment K, Cost Reply (Price Workbook).** The SD-WAN Service must provide secure access to data resources within MFN-3 by extending any L3VPN service supported as well as secure centralized internet services.

Costs associated with SD-WAN services cannot be billed as part of the “core port” service charges; they must be independent of the MFN-3 Core Network port service charges. The Services Provider should propose a rate structure that amortizes the SD-WAN infrastructure equipment and associated hardware/software that supports the integration of the SD-WAN solution with the MFN3 core. The SD-WAN appliance using the CPE formula and SD-WAN configuration management fee in the price workbook shall be used to recover any costs associated with the SD-WAN infrastructure build-out and management.

These specifications may not list all equipment or software required to produce an operational SD-WAN Service. The reply must contain a complete service solution with all necessary components and ongoing maintenance/support/licensing. The Services Provider will be responsible for verifying all components are compatible when integrated with MFN-3 and Customer systems.

The MFN-3 SD-WAN Service must utilize strong authentication and encryption including Advanced Encryption Standard (AES) with a minimum of 256-bit keys for data encryption. AES-256 is widely recognized for its strong security and performance. The service must ensure that all control plane traffic is encrypted using protocols such as DTLS (Datagram Transport Layer Security) or TLS (Transport Layer Security). The SD-WAN service shall provide end-to-end encryption to protect data from the source to the destination, ensuring that data remains secure throughout its journey across the network ensuring that encryption is applied to both data plane and control plane traffic.

There are numerous components to be integrated together as part of the SD-WAN service. As SD-WAN is an end-to-end service, the Services Provider is responsible for the installation, day-to-day troubleshooting, issues resolution, and administration of all related components. The Services Provider is required to coordinate all activities associated with related equipment installations, including coordinating inside wiring installation as required.

Provide responses to the following requirements:

- **Solution Overview**: Provide a detailed description of the proposed SD-WAN solution, including architecture, key features, and benefits.
- **Implementation Plan**: Outline the implementation process, including timelines, milestones, and resource requirements.
- **Security Features**: Describe the security measures integrated into the SD-WAN solution to protect against cyber threats and ensure data integrity.
- **Encryption Standards**: Use of AES-256 for data encryption and DTLS/TLS for control plane traffic.
- **End-to-End Encryption**: Protection of data from source to destination.
- **Encryption Key Management**: Automated key management systems with regular key rotation.
- **Data Integrity and Authentication**: Mechanisms to ensure data integrity and strong authentication methods.
- **Compliance with Security Standards**: Adherence to FIPS 140-2 and other relevant security standards.

- **Performance Metrics**: Performance metrics and Service Level Agreements (SLAs) that will be used to measure the effectiveness of the solution are described in the SLA section of this procurement.
- **Scalability**: Explain how the solution can accommodate future growth and changing network demands, including the ability to handle thousands of remote site connections for multiple agencies and stakeholders.
- **Geo-Redundancy and Resiliency**: Detail the redundancy and resiliency features of the SD-WAN Infrastructure including:
    - High availability configurations to ensure continuous operation.
    - Failover mechanisms to maintain connectivity in case of hardware or network failures.
    - Disaster recovery plans to quickly restore services in the event of a major outage.
- **Multi-Tenancy**: Describe how the solution supports multi-tenancy, including:
    - Isolation of data and network traffic between different agencies and stakeholders.
    - Customizable policies and configurations for each tenant.
    - Management and reporting capabilities for individual tenants.
- **Management and Support**: Detail the management tools and support services provided, including 24/7 help desk support and network monitoring.

2.20.1 Installation, Monitoring, and Trouble Reporting for SD-WAN

It is the Services Provider's responsibility to coordinate with the Customer to facilitate and successfully establish connectivity. The Services Provider must monitor each SD-WAN connection.

As needed, the Services Provider is required to coordinate a conference call with DMS and the MFN-3 Customer to turn up and test the SD-WAN connectivity. DMS will act as an escalation point for any problems that may arise if the Services Provider encounters any cooperation issues.

The Services Provider is required to immediately notify the DMS NOC, and the affected MFN-3 Customer when an SD-WAN connection goes down or is not functioning correctly. The Services Provider's NOC is required to open a trouble-ticket to document the SD-WAN issue and take necessary corrective actions.

Installation, monitoring, and trouble reporting are inherent features of MFN-3 so there is no specific entry within Attachment K, Cost Reply (Price Workbook).

Provide a description of the monitoring process if the standard MFN-3 tools suite cannot be used.

Discuss any limitations using the MFN-3 tools suite in this application. In addition, describe the proposed trouble-reporting process.

2.20.2 Contractor Provided SD-WAN CPE Appliance

The Services Provider will be responsible for providing the SD-WAN edge appliance. The device shall be installed at the Customer location and assume end-to-end responsibility for elements of the service to include the hardware appliance, installation, maintenance, and software configuration. The Services Provider is

responsible for deploying SD-WAN devices throughout the State of Florida at no cost other than those listed in Attachment K, Cost Reply (Price Workbook). Include a design narrative with diagrams as needed that describes the proposed plan to address the requirements of the subsection. Discuss the proposed plans to accomplish the requirements for in state and out-of-state installations.

Enter the appropriate costs in Attachment K, Cost Reply (Price Workbook), SD-WAN.

2.21 SASE Secure Access Service Edge

This can be delivered either through a dedicated or commercial solution.

A Secure Access Service Edge (SASE) will be provided as an optional service to Customers, delivering a cloud-based framework that combines network connectivity functions with various security services including, but not limited to Cloud Access Security Broker (CASB), antivirus, Zero Trust Network Access (ZTNA) and Firewall as a Service (FWaaS).

Costs associated with SASE cannot be billed as part of the "core port" service charges; they must be independent of the MFN-3 Core Network port service charges. SASE orders shall be priced on an individual case basis.

The solution should deliver:

- Flexible, scalable licensing model to support rapid endpoint expansion.
- Integration with Cloud Identity and Access Management Solution for Authentication, Authorization, and Accountability (AAA) requirements combined with Location, Device, and Behavioral monitoring to support Zero-Trust architecture.
- Ability to resist or prevent user tampering (e.g. UI password protection).
- Ability to alert on unauthorized configuration changes.
- Integration with Security Incident Event Management (SIEM) Platforms using either Syslog or API.
- Capacity and Availability Monitoring with ability to set system alarms, thresholds, and send notifications using SMTP, Syslog, or API.
- Able to perform detailed activity reporting based on user(s), groups, applications, or sites.
- Health reporting and remote installation capability to manage endpoint lifecycle (new, edit, retire)
- Security threat detection and response to identity suspicious events and block malicious events.
- URL/web policy based on connected user(s) and groups for both internal and external networks.
- Replacement of network-level VPN access with application-level, context-aware, identity-based access ZTNA (Zero Trust Network Access).

Describe the SASE solution that will be made available as part of the MFN-3 Core Services:

Solution Overview: Provide a detailed description of the proposed SASE solution, including architecture, key features, and benefits

- Implementation Plan: Outline the implementation process, including timelines, milestones, and resource requirements
- Security Features: Describe the security measures integrated into the SASE solution to protect against cyber threats and ensure data integrity
- Performance Metrics: Performance metrics and Service Level Agreements (SLAs) that will be used to measure the effectiveness of the solution are described in Attachment C, Service Level Agreements.
- Scalability: Explain how the solution can accommodate future growth and changing network demands.
- Redundancy and Resiliency: Detail the redundancy and resiliency features of the SASE solution, including high availability configurations to ensure continuous operation, failover mechanisms to maintain connectivity in case of hardware or network failures, disaster recovery plans to quickly restore services in the event of a major outage.
- Multi-Tenancy: Describe how the solution supports multi-tenancy, including isolation of data and network traffic between different agencies and stakeholders, customizable policies and configurations for each tenant, and management and reporting capabilities for individual tenants.
- Management and Support: Detail the management tools and support services provided, including 24/7 help desk support and network monitoring.
- Provide a list of SLAs for SASE service that covers the end-user and Infrastructure for availability and performance degradation. The Services Provider description must include the proposed values for performance target and service credits along with the measurement criteria. The Respondent should use the same layout as **Attachment C- Service Level Agreements.**

2.22 Cloud Transport

This can be delivered either through a <u>dedicated or commercial solution</u>.

MFN-3 Cloud Transport Services provides connectivity between a supported cloud service provider and MFN-3, allowing MFN-3 Customer sites to access cloud service providers using their private, common, or public VRFs Cloud Transport Services are to be provided via Ethernet Virtual Connections (EVC's). The Services Provider must provide access to individual cloud service providers by way of a primary EVC for each Customer per cloud service provider per VRF on a primary dedicated connection. The Services Provider must also provide a secondary EVC per Customer per cloud service provider on a dedicated connection that is separate from the primary dedicated connection. The secondary EVC shall ensure continuity of service for each Customer if the primary EVC fails. Automatic failover will be handled via dynamic routing protocols between MFN-3 core nodes.

Using Cloud Transport Services, Customers will be able to establish connections to cloud services providers. The Services Provider will provide EVC's between Customers and cloud service providers at the following bandwidth:

- 50Mbps
- 100Mbps
- 200Mbps

- 500Mbps
- 1000Mbps
- 2000Mbps
- 5000Mbps
- 10000Mbps

The Services Provider must establish multiple diverse NNI peering links to be used to support Cloud Transport Services. The Services Provider must manage and monitor all NNI links and all Customer EVC's. The Services Provider will be the single point of contact for any trouble, isolation and resolution for Cloud Transport Services. SLA's have been established in **Attachment C – Service Level Agreements**, in the Cloud Transport Services section for Customer EVC availability.

Describe the Cloud Transport Services that will be made available on the MFN-3 contract.

2.23 Ancillary Network Services – General

For all the subsections below, enter rates in Attachment K, Cost Reply - Ancillary Network Services. An MFN-3 eligible user must subscribe to an MFN-3 network service such as WAN or VPN to MFN-3 in order to qualify for subscribing to Ancillary Network Service.

2.23.1 Telecommunication Service Priority

Telecommunication Service Priority (http://tsp.ncs.gov) is a program that authorizes national security and emergency preparedness (NS/EP) organizations to receive priority treatment for vital voice and data circuits or other telecommunications services. As a result of hurricanes, floods, earthquakes, and other natural or man-made disasters, telecommunications service providers frequently experience a surge in requests for new services and requirements to restore existing services. The Telecommunication Service Priority Program provides telecommunication service providers an FCC mandate to prioritize requests by identifying those services critical to NS/EP. It shall be the responsibility of the Customer to request the Telecommunication Service Priority Services and provide the Customer's Telecommunication Service Priority Authority Code to the Services Provider.

2.23.2 Demarcation Extension Service

Demarcation extension service must include the necessary equipment, wiring, cables, inspection, and installation in order to extend the demarcation, per MFN-3 Customer requirements. The Services Provider shall be responsible for maintaining and managing the demarcation extension for the life of the contract at no additional cost to the State. There will be no Demarcation Extension Service charges permitted for any sites migrating from MFN-2 to MFN-3. The Services Provider will be responsible for migrating these current services at no cost. However, for new sites, the Services Provider will be permitted to charge for Demarcation Extension Services as authorized by DMS. MFN-3 Customers have the option to utilize the SUNCOM Telecommunications Infrastructure Project Services (TIPS) contract for such services.

2.23.3 After-Hour Installation Services

Provide After-Hour Installation Services between 5:01PM and 11:00PM & between 5:00am and 7:59am local time Monday through Friday, with pricing set at the same rate for both after-hour installation blocks. Holiday and weekend support for installation shall be provided with pricing on an ICB basis.

There will be no After-Hour Installation Service charges permitted for any sites that migrate from MFN-2 to MFN-3; these sites will be subject to the Migration SLA in **Attachment C – Service Level Agreements**. For new sites, the Services Provider shall be permitted to charge for After-Hour Installation Services as authorized by DMS.

2.23.4 Expedited Installation Services

Expedited installation shall allow Customers to receive an installation before the normal installation intervals defined in the **Attachment C – Service Level Agreements**. If the expedited service due date on the approved DMS work order is not met, the Services Provider shall not charge for expedite services. The Services Provider is not permitted to charge higher than the cost specified on the approved DMS work order. Attachment K, Cost Reply contains the table with the number of days the installation date can be advanced (improved), and the related fee to be paid by the Customer .

There will be no Expedited Installation Service charges permitted for any sites that migrate from MFN-2 to MFN-3; these sites will be subject to the Migration SLA in **Attachment C – Service Level Agreements**. For new sites, the Services provider shall be permitted to charge for Expedited Installation Services as authorized by DMS.

The Services provider is required to migrate sites as specified in, **Attachment C – Service Level Agreements**. Expedited installation fee would not apply to the Services provider's efforts as they migrate sites to the MFN-3 infrastructure.

2.24 Miscellaneous Conditions

The reply to this Section and each of its subsections is:

"Respondent has confirmed they have read, understands, and will comply with the statements contained in this subsection."

2.24.1 No Cost Increase

Costs shall not increase for any MyFloridaNet-3 service for the life of the contract.

2.24.2 Third Party and/or Independent Charges

All rates in the Price Sheets are inclusive of any third party and/or independent company local loop access charges.

2.24.3 Florida Administrative Code

The Services Provider shall also adhere to the terms and provisions as set forth in the following chapters of the Florida Administrative Code, while delivering/providing the Services under this solicitation. See Div. 60FF: Technology Program - Florida Administrative Rules, Law, Code, Register - FAC, FAR, eRulemaking. and Div. 60GG:

Florida Digital Service - Florida Administrative Rules, Law, Code, Register - FAC, FAR, eRulemaking

- 60FF-1: State Communications Definitions; Usage, Qualification; Exemptions and Clearances
- 60FF-2: State Communications Order Processing and Billing
- 60FF-3: State Network Usage and Security
- 60GG-1: Department of Management Services Project Management and Oversight
- 60GG-2: State of Florida Cybersecurity Standards
- 60GG-3: Data Center Operations
- 60GG-4: Cloud Computing
- 60GG-5: State of Florida Enterprise Architecture
- ADA Compliance: All tools are to be ADA compliant.

2.24.4 No One-Time or Non-Recurring Charges

There shall be no one-time, or non-recurring charges such as installation, disconnect, cancellation, or work order fees unless otherwise expressly stated by DMS in the Price Workbook. For example, there must not be an install charge if a Customer wants to upgrade CPE to obtain a second Ethernet port. There will be no charge for rolling the trucks or sending a technician to upgrade the CPE. Similarly, there will be no charge to upgrade CPE software (either remotely or a visit to the site) to meet the standards of the service (CPE or access).

There must not be any installation charge when Customers want to:

- Upgrade their managed CPE.
- Upgrade their Customer-owned CPE that is Customer-managed.
- Change their access (local loop).

2.24.5 Proposed Equipment (CPE and MFN-3 Services Infrastructure)

Respondents must not propose equipment that is announced End-of-Sale, End-of Support or End-of-Life by the equipment manufacturer. Respondents should propose only new equipment in support of the MFN-3 services.

2.24.6 Services provider Responsibility for Infrastructure Upgrades

As a managed service, the Services Provider is responsible for keeping up with the MyFloridaNet-3 Services Infrastructure to meet business/technical SLAs and Customer requirements such as bandwidth upgrades and new connections, at no cost to the State.

2.24.7 Engineering Support

DMS engineering staff shall receive full design and engineering support from the Services Provider for all engineering and design matters throughout the life of the contract.

2.24.8 CPE Configuration Templates for Customer Managed CPE

The Services Provider will provide standard CPE configuration templates for Customers to utilize, enabling their equipment to effectively interface with the MFN-3 Core Network.

2.24.9 Operational Change Request Process

The Department may authorize operational changes to services and infrastructure that do not have a pricing impact (non-billable changes). These operational changes do not require a Contract amendment, but will be memorialized in writing, upon the Department's contract manager's approval.

However, DMS reserves the sole right to make the final determination if a change request or Contract amendment is required. Updates to the Certified CPE List are defined by the CPE formula and are deemed to be operational changes.

Pricing related changes require a Contract amendment pursuant to paragraph 42 of the Special Conditions within **Attachment B, Draft Contract**. A change which would allow the Services Provider to offer less of any deliverable under the Contract, which may include commodities, services, technology, or software, requires a Contract amendment.

2.24.10 Authentication Server and Logs

All vendor-managed MFN-3 equipment must authenticate with the Services Provider's authentication server. DMS must be provided with access to the Services Provider's authentication logs.

Access to logs for audit purposes is to be provided.

2.24.11 Using Standards and Templates

Engineering and administrative processes will be built around standards and processes. For example, a common security strategy and service template for the overall network is required; SNMP password assignments and related configurations will follow standards. Initial standards for engineering will be documented in the MFN-3 Services Infrastructure Plan. Additional standards and operational procedures for (for engineering and administrative processes) will be updated in monthly meetings and placed in the user and operations guides. Use of template engine or automated tools is strongly encouraged but not required to improve efficiency and accuracy of templates and configurations.

2.24.12 Customer Responsibilities for On-Site Contact Information

When trouble occurs and an on-site visit to the Customer premises is required to replace CPE, the Customer must provide a live on-site contact that will be at the Customer premises to receive replacement CPE and/or to allow the MyFloridaNet-3 technician access to the site. Regardless of the success or failure of contacting an on-site Customer representative, the Services Provider's NOC will troubleshoot, particularly circuit issues, to the fullest extent possible.

2.24.13 Single Point of Contact

The Services Provider shall designate an account manager to act as the single point of contact for all DMS issues. The Services Provider shall also designate a single point of contact for each local loop provider through the subcontractor information form.

2.24.14 Non-Contiguous IP Address Blocks

The State's intranet contains non-contiguous IP address blocks. The Services provider will work with DMS to engineer routing to respond to BGP announcements and other DMS firewall issues involving those non-contiguous addresses.

2.24.15 Urgent Bandwidth Increase

There are times when a site requires an urgent bandwidth increase. In this case, an exception to the normal provisioning process will be made to provide the requested bandwidth in an abbreviated timeframe when both installed bandwidth and CPE allow such immediate changes. The minimum expedite charge as specified in the Price Workbook will be required of the Customer.

2.24.16 Network Management System updates

The implementation process must populate a new device into the Network Management System Tools within two business days after formal Customer acceptance of service.

2.24.17 Turn-Up Support for Customer-Provided CPE

Turn-up of services shall be available for Customer-provided and Customer-managed CPE. The Services provider shall be responsible for being on-site to turn-up the service for Customer-provided and Customer-managed CPE at no additional charge. However, Customer shall be responsible to configure (if CPE configuration management option is not selected) and installation of Customer-provided CPE. Turn-up support also applies when CPE is being replaced due to maintenance issues.

2.24.18 SUNCOM or MFN-3 Brand

The look and feel of MyFloridaNet-3 Customer facing services shall have the SUNCOM or MyFloridaNet-3 brand where possible.

2.24.19 MFN-3 Marketing Initiatives

The Services provider will be responsible for marketing MyFloridaNet-3's portfolio of services to Customers and for drafting the content for the SUNCOM website. Marketing initiatives shall always reflect DMS as the service provider. DMS will review and approve the content. DMS may, at its sole discretion, opt to handle these initiatives at any point during the contract if deemed to be in the best interest of the State.

2.24.20 Acceptance Criteria

The date of acceptance is the date the Customer accepts the services as installed and in good working order. The Customer will certify in CSAB when the service has been accepted.

2.24.21 Criteria for IMAC Signoff and Billing Start

The following criteria must be met before operational IMAC is considered complete.

- Respondent completes all requirements detailed in the CSAB work order
- The Customer will certify acceptance of service in CSAB
- The service has been populated in the MFN-3 Network Management System
- The CSAB work order has been closed by the Services provider in CSAB by entering a completion date and effective bill date. As part of closing the work order, additional required closeout information must be entered in the CSAB Order Closeout Information section of the work order.
- All dates in CSAB must be entered by the Services provider in real time; CSAB system does not permit a date entry to be backdated.
- The Services provider is responsible for the cost of the services for any loss of E-rate funding due to Services provider violation of the Timely Invoicing SLA.
- Billing starts once the operational IMAC signoff criteria is complete unless the live test period applies.

2.24.22 Bill Stop Date

Billing shall stop for any type of service disconnects as indicated by DMS on the disconnect CSAB order. The bill stop date shall be the same day the Services provider receives the disconnect CSAB from DMS or the bill stop date as specified by DMS on the disconnect order. The bill stop date shall be on or after the date the order is received by the Services provider.

2.24.23 Invoices

Invoices to DMS must reflect only those commodities listed in the catalog.

2.24.24 Guaranteed Bandwidth Speed

Bandwidth speed listed in the Price Workbook must be guaranteed for components such as the MFN-3 core port and Internet Access.

2.24.25 Month-to-Month Term

All services and any components of the service shall be available on a month-to-month term basis except where expressly stated by DMS. No termination liabilities are associated with any service provided under this contract.

2.24.26 Operational Guide

The Services provider is responsible for developing, maintaining and updating operational guide. The Operational Guide is intended to be a set of instructions on the operational and business aspects of the various services.

2.24.27 Quantity or Revenue Guarantees

There are no quantity commitments or revenue guarantees associated with any service provided under this contract.

2.24.28 Published Rates Include the DMS Administrative Fee

The rates in Price Workbook are considered wholesale and will ultimately be marketed to Customers with the DMS administrative fee. The Services provider must advertise only the rates that include the DMS administrative fee.

2.24.29 Statewide Uniformity

Pricing and services shall be available statewide except where expressly stated by DMS.

2.24.30 Standard Operating Procedures

The Services Provider will make their MFN-3 standard operating procedures and any other MFN-3 documentation available to DMS upon request.

2.24.31 No Upfront Costs to DMS for the Implementation of the MFN-3 Infrastructure

DMS will not pay any upfront MFN-3 Services Infrastructure costs. The MFN-3 Services Infrastructure includes but is not limited to MFN-3 core backbone facilities, MFN-3 core infrastructure, Internet Gateway equipment, firewalls, staffing, MFN-3 NOC, NMS tools, VPN services, SD-WAN services, and licenses. DMS shall only pay the Services Provider when new sites and services are installed and begin to operate successfully per the rates and services in **Attachment K, Cost Reply (Price Workbook)**.

2.24.32 Travel

There will be no travel reimbursements.

2.24.33 Labor

Labor required to make configuration changes to the MFN-3 Services Infrastructure is an inherent component of supporting MFN-3. Any implementation of features, functionality, or configuration changes associated with MFN-3 will be configured at no cost to DMS and its Customers. Changes can be made after-hours at no cost.

2.24.34 Enable Features, Functionality and Configuration Changes

At the sole discretion of DMS, the Services Provider shall enable any features, functionality or configurations that are supported by any equipment or systems manufacturer under MFN-3 at no cost to DMS or its Customers.

2.24.35 Connections/Links Utilization

Where dedicated, any MFN-3 Services Infrastructure connections/links including but not limited to backbone links, transit links, aggregate links, Cloud Transport Service links, links between any devices or systems will not exceed 60% average utilization between 8AM to 5PM for five (5) consecutive business days. If the utilization goes above 60%, the Services Provider will upgrade these connections/links to normalize usage to 60% or below within 30 calendar days at no cost to DMS or its Customers. Transit links are subject to this utilization requirement for both dedicated and commercial deployments. Performance and monitoring tools shall constantly monitor for connection/links usage and provide email alerts to DMS if thresholds are exceeded over 60%. The Services Provider shall be subject to the SLA related to

Connections/Links Utilization as specified in **Attachment C, Service Level Agreements**. Core infrastructure backbone and aggregate links should be sized based on subscribed services outlined in **Attachment K, Cost Reply Price Workbook** Tab 11 – Site Inventory, column M represents the access/core port speed subscribed to for WAN inventories indicated in column I. Transit link sizing should be based on subscribed internet services outline in in **Attachment K, Cost Reply Price Workbook** Tab 11 – Site Inventory, with speeds indicated in column M and internet subscription indicated in column J.

2.24.36 NMS and Security Tools Metric Alerts

Where dedicated and available, any components that make up the Network Management Systems and Security Tools shall be monitored by the Services provider for metrics including but not limited to CPU utilization, Memory Usage, Disk Usage, Uptime. At DMS sole discretion, the parameters for these metrics shall be established during MFN3 Services Infrastructure implementation.

2.24.37 Delivery of All Services

The Services provider must deliver all services priced in the Price Workbook except for End of Sale CPE.

2.24.38 Final Determination

DMS will make the final determination on contract compliance.

2.25 Project Management

As described in section 2.24.3 of this SOW, the Service Provider shall adhere to the terms and provisions as set forth in the Florida Administrative Code while providing the Services under this solicitation. Relevant provisions and code references are listed in section 2.24.3.

Included within those requirements, the Services provider must provide project management services in accordance with Rule 60GG-1.004 Planning, and any later modification or amendment of the rule. The matrix provided in Rule 60GG-1.004 lists planning activities and documents required for the project based on the project's Risk and Complexity (R&C) Category. Documentation listed in the matrix within 60GG-1.004, whether created separately or combined as a single document, constitutes the Project Management Plan. Requirements of similar plans and planning documents referenced throughout this SOW shall also be satisfied to the extent they are not inconsistent with the requirements set forth in in Rule 60GG-1.004.

All project schedules, including the Project Management Implementation Schedule, must be submitted as Microsoft Project (mpp) files. All other Project Management documents must be submitted as either a Microsoft Word 2021 (or higher) document, or Adobe pdf. All project management documents will be submitted to the DMS Contract Manager.

For all of Section 2.25¸ describe in detail how the Respondent will provide project management in accordance with the minimum requirements listed.

The following subsections contain the minimum requirements for Project Management:

2.25.1 Project Charter and Project Management Plan

The Project Charter is a deliverable subject to final acceptance by DMS. The Services provider must submit an acceptable Project Charter within four weeks of the Contract execution.

- Minimum Acceptance Criteria: The Project Charter must formally authorize the existence of a project and provide the DMS and Contractor's Project Manager with the authority to apply organizational resources to project activities. The deliverable must meet the Project Risk and Complexity Category 4 requirements of Rule 60GG-1.002, F.A.C.

The Project Management Plan is a deliverable subject to final acceptance by DMS. The Services provider must submit an acceptable Project Management Plan within 4 weeks of the Contract execution.

- Minimum Acceptance Criteria: The Project Management Plan is the document that describes how the project is monitored, controlled, and executed. The deliverable must meet the Project Risk and Complexity Category 4 requirements of Rule 60GG-1.002, F.A.C.

The plans listed below may be considered as additional components of the Project Management Plan. However, DMS considers these plans listed below as deliverables separate from the Project Management Plan.

- Readiness Plan is a deliverable subject to final acceptance by DMS. The Services provider must submit an acceptable Readiness Plan within six weeks of the Contract execution.
- Minimum Acceptance Criteria: The Services provider must deliver a detailed organizational readiness strategy and associated plans that outline a readiness methodology, approach, activities, dependencies, and assumptions for key stakeholders to successfully support project activities.

Communications Management Plan is a deliverable subject to final acceptance by. The Services provider must submit an acceptable Communications Plan within six weeks of the Contract execution.

- Minimum Acceptance Criteria: The Services provider must develop a Communications Management Plan that defines all communication touch points between the Project and all impacted stakeholders. The deliverable must meet the Project Risk and Complexity Category 4 requirements of Rule 60GG-1.002, F.A.C.

Risk Management Plan is a deliverable subject to final acceptance by DMS. The Services provider must submit an acceptable Risk Management Plan within six weeks of the Contract execution.

The Requirements Management Plan is a deliverable subject to final acceptance by DMS. The Services provider must submit an acceptable Requirements Management Plan within six weeks of the Contract execution.

- Minimum Acceptance Criteria: The Services provider is responsible for managing all business requirements, including confirmation, design, development, testing, and validating that they are ultimately met during implementation. The Services provider's Project Manager will work with DMS to develop and administer a plan to effectively manage requirements throughout the Project.

The Disaster Recovery Plan is a deliverable subject to final acceptance by DMS. The Services provider must submit an acceptable Disaster Recovery Plan within three months of the Contract execution.

- Minimum Acceptance Criteria: The Services provider must deliver a detailed Disaster Recovery Plan and associated plans that outline disaster recovery methodology, backup procedures, recovery plan, restoration plan, rebuilding process, testing of the disaster recovery plan and record of plan changes. The plan will include the following at minimum:
  - Plan Objectives.
  - Assumptions.
  - Definition of Disaster.
  - Recovery Teams.
  - Team Responsibilities.
  - Internal and External Communications.
  - Federal, State, Local Roles and Responsibilities.
  - Services Restoration.
  - Support Timeline.

2.25.2 Project Management Implementation Phase

The Project Implementation Phase starts after the acceptance of the Project Charter and ends with the DMS acceptance of a completed Services Infrastructure Checklist.

Project Management Implementation Phase Schedule is a deliverable subject to final acceptance by the Department. The Services provider must submit an acceptable Project Management Implementation Phase Schedule to the DMS Project Manager every two weeks by noon ET on Fridays. The document must be baselined, be resource loaded with predecessors, successors, durations, costs, and calculated earned value metrics Cost Performance Index (CPI) and Schedule Performance Index (SPI) and updated every two weeks as needed until the completion of the Project Implementation Phase. This should be accompanied with a narrative which includes the current status of the project, actions that have taken place in the last two weeks, any new risks and their associated risk mitigation plans, any new issues, and any tasks more than then percent (10%) behind schedule and a plan to complete the task.

- Minimum Acceptance Criteria: Create and maintain a Microsoft Project 2016 (or higher) schedule to incorporate all project activities to the agreed upon work breakdown structure level. The schedule must include at a minimum: task durations, start and finish dates (baseline and actual), predecessors and successors, resources, deliverables, and milestones, and calculate CPI and SPI earned value metrics. The deliverable must meet the Project Risk and Complexity Category 4 requirements of Rule 60GG-1.002, F.A.C.

Project Management Tracking Logs (Risks, Issues, Action Items, Decisions, and Operational Changes requested) are deliverables that are first due two weeks following the Project Kickoff Meeting, and shall be due every two weeks thereafter, until the completion of the Project Implementation Phase. These are updated as necessary, as determined by the Services provider and DMS.

- Minimum Acceptance Criteria: The Services provider must identify, assess, document, and recommend mitigation strategies by updating and submitting to DMS the tracking logs at a minimum of bi-weekly to reduce project risks and issues. The deliverable must meet the Project Risk and Complexity Category 4 requirements of Rule 60GG-1.002, F.A.C.

Project Status Report is a deliverable subject to final acceptance by DMS. The Services provider must submit an acceptable Project Status Report to DMS. This deliverable is first due within two weeks of the Project Kickoff Meeting after Contract execution, and shall be due weekly thereafter, until completion of the Implementation Phase.

- Minimum Acceptance Criteria: The Services provider must provide weekly Project Status Reports which are due via email to the DMS Contract Manager each Thursday by 5 PM Eastern time, and must include:
  - A narrative description of significant project activities that have been conducted or are underway.
  - The progress-to-date on project activities.
  - An explanation of any tasks/activities that are behind schedule and a plan to bring them current.
  - Notification of issues or risks that have been encountered and their resolution or plan for future resolution.
  - Upcoming deadlines.

2.25.3 Project Management - Guides

The Services provider shall create the following guides. These guides are deliverables subject to final acceptance by DMS. The Services provider must submit acceptable guides to DMS within three (3) months of Contract execution and will be updated as necessary during the Contract term. The guides are subject to the final acceptance of DMS.

- MFN-3 Services Infrastructure Operations Guide - The Services provider shall create a MFN-3 Services Infrastructure Operations Guide. This will include engineering, operational, and business processes for service delivery. At a minimum, the guide includes ordering, trouble reporting, SLA monitoring, and invoicing processes.
- MFN-3 Services Infrastructure User Guide - The Services provider shall create an MFN-3 Services Infrastructure User Guide, intended to provide a set of instructions for the Customer on how to use the services.
- MFN-3 Services Infrastructure System Administration Guide - The Services provider shall create an MFN-3 Services Infrastructure Administration Guide for Customer s and describe all administration processes for service delivery.

2.25.4 Project Management - Closure

The Services provider shall create project closure documentation. This deliverable is due to DMS one (1) month from the close of the Project Implementation Phase.

- Minimum Acceptance Criteria: The project closure documentation must include a lessons-learned document, final schedule, and retrospective of the project.

2.25.5 Project Management Implementation and Migration Plans

Implementation Plan is a deliverable subject to final acceptance by DMS. The Services provider must submit an acceptable Project Management Plan to DMS within six weeks of the Contract execution. The Implementation Plan will address all activities in the Project Implementation Phase, which starts after the acceptance of the Project Charter and ends with the DMS acceptance of a completed Services Infrastructure Checklist.

- Minimum Acceptance Criteria: The Services provider must deliver a detailed Implementation Plan that outlines an implementation, approach, activities, dependencies, and assumptions for key stakeholders to support a successful project implementation. Furthermore, the Implementation Plan shall include at a minimum:
    - Schedule of activities.
    - Resource allocation.
    - Implementation and migration preparation planning and impact analysis.
    - System build out.
    - Acceptance.
    - Migration cutover.
    - Fallback to previous service.
    - Interface with CSAB for billing and ordering.
    - Interface with MFN (Network-to-Network Interface, day-to-day operations, and security).
    - Network support.
    - Operations Centers (NOC and SOC).
    - Day-to-day operational support services.
    - Training – cross reference training section.

Individual Customer Specific Migration Plans: The Services provider will be responsible for creating Individual Customer Specific Migration Plans as each existing and new Customer migrates to the MFN-3 Services Infrastructure. Additionally, a migration plan may be required if a Customer undertakes a significant or complex change in how it operates under the MFN-3 Services Infrastructure. The Individual Customer Specific Migration Plans are deliverables that must be developed in coordination with the Customer and are subject to the acceptance of DMS and the Customer. These Individual Customer -Specific Migration Plans will vary based on the proposed service and the complexity of the service migration. The Services provider must submit plans acceptable to DMS and the Customer within four (4) weeks of receipt of a written notification of the plan's requirement from DMS to the Services provider. Furthermore, the Individual Customer Specific Migration Plans shall include at a minimum:

- Schedule of activities, which is consistent with the Project Implementation Phase schedule.
- Resource allocation.
- Migration and preparation planning.
- Impact analysis.
- Stakeholder communications plan.
- Migration management.
- Engineering.
- System build out.
- Acceptance (phase/final).
- Migration cutover.
- Fallback to previous service.
- Day-to-day operational support services.
- Training – cross reference training section.

SECTION 3.0 *Performance Measures (Service Level Agreements - SLAs)*

3.1 Performance Measures

Service Level Agreements Introduction: MyFloridaNet-3 will provide network performance, service delivery, and operational service level commitments to meet performance requirements. These commitments shall be based upon guaranteed restoral times and other performance measures, with associated service credits for Services provider's non-compliance.

Attachment C - Service Level Agreements, consists of:

- SLA requirements.
- Performance target and related numeric value.
- Financial consequence for non-performance.
- SLA details, measurement and performance criteria.
- Service applicability.

3.1.1 SLA Criteria

The term "SLA performance monitoring service" is used to indicate a system that receives information on outages, degradation and other SLA requirements, then provides notifications to Customer s and opens SLA related tickets. The Statement of Work does not specify how the SLA performance monitoring service interfaces with other network tools or functions that provide network monitoring and network management. The narrative describing the actual SLA tool (system) is to be provided in subsection 2.16.19: Proposed SLA Performance Monitoring Service Functionality.

In addition to **Attachment C, Service Level Agreements** listed below are requirements associated with MyFloridaNet-3 SLAs. **Any qualification, exception, counteroffer, edit, or deviation to an SLA is not allowed in this response.** DMS is open to discussing SLAs that provide better value to the State as part of contract negotiations.

- Where applicable, FSLAs will be addressed on a per circuit basis.

- For SLAs the respondent needs to outline their SLA testing methodology with details around the testing parameters and calculation methods.
- The Services provider is required to provide and comply with SLAs defined in Attachment C.
- Unless there is an explicit reference to “weekdays” or “business days,” all SLAs, service credits and IMAC windows are applicable based on calendar days.
- Tickets based on phone calls or emails from DMS and MFN-3 Customer s are to be opened by the Services provider’s NOC staff immediately.
- Each month the Services provider and DMS shall scrub all data related to SLAs for both On-net and Off-net services. Based on this scrub, credits shall be provided to DMS by the Services Provider. Customers are not required to explicitly request or otherwise initiate the SLA scrubbing and validation process in order to receive SLA credits.
- Violation of performance measure thresholds in the SLAs will result in service credits to DMS as appropriate. Service credits must be explicitly identified as a line item to DMS on the Services Provider’s monthly invoice.
- SLAs have no monetary cap.
- If a single incident results in failure to meet multiple SLAs simultaneously, the service credits associated with such failures shall not be cumulative. Instead, DMS shall be entitled to service credits representing the greatest monetary value among all triggered SLAs for that specific incident.
- To support the SLA process, DMS shall have access to the supporting raw data for the Services provider; there shall be no restriction on content. DMS shall have access to 100% of the raw data.
- Operational IMAC for CPE configuration changes shall be initiated through the Respondent's trouble ticketing system.

The MFN-3 Services Infrastructure and site migration efforts must be accepted by DMS within the applicable performance target if the Services provider is to avoid having to provide DMS with service credits.

All required tasks on the MFN-3 Services Infrastructure checklist listed below must be implemented, successfully tested, or otherwise approved by DMS before the Services provider is permitted to migrate any sites to the MFN-3 infrastructure. The checklist is the set of requirements defined within the Statement of Work. The Services provider shall not be permitted to migrate any sites until the Services provider completes all tasks in the checklist and the completion has been accepted by DMS, the date of which will constitute the “Services Readiness Date.” The targeted Services Readiness Date is defined in the SLAs.

The MFN-3 Services Infrastructure checklist includes but is not limited to:

- Plan, design, implement, and deploy services such as core equipment, backbone facilities, security functionality, NetFlow, Remote access functionality, and Internet gateway (including gateway firewall services).
- Implement and deploy Network Management Systems tools.
- Develop training material on how to use Network Management System tools.
- Develop the MFN-3 Services Infrastructure Build-out Plan.

- Detail project and migration plans covering both MFN-3 Services Infrastructure rollout and end-site migration.
- Establish adequate staffing to accomplish the migration of end-sites and completion of the MFN-3 Services Infrastructure checklist. This includes the project management team.
- Schedule initial meetings with Customer s to start discussions related to the migration and timeline.
- Implement a process for streamlining scheduling of migration tasks with Customer s, with a focus on addressing potential issues such as point-of-contact unavailability or unresponsiveness.
- Provide adequate staffing and training to the Services provider's staff including Network Operations Center.
- Implement SLA measurement systems and processes.
- Develop a detailed SLA scrubbing and validation process.
- Per the business operations section, implement the interface between CSAB and the Services provider's billing system to fulfill requirements for ordering and billing processes. All requirements in the business operations section must be completed. As successful mock bill must be completed.
- Finalize the equipment Certified CPE List.
- Implement systems and services for remote access VPN.

Two weeks before the MFN-3 Services Infrastructure is approved for production, DMS shall refresh the current network Site Inventory to create a final Site Inventory.

The MFN final Site Inventory allows DMS and the Services provider to decide as to which SLA is applicable: the MyFloridaNet-3 Operational IMAC SLA or the Migration of MFN sites SLA. Operational IMAC SLAs shall not apply to the final Site Inventory during the migration window, because those sites are governed by the per-day SLAs on the migration of all sites to the new MFN-3 contract.

The SLA clock must not restart but can be suspended (hold time) for approved reasons agreed on between DMS and the Services provider. During the monthly operational meetings, DMS shall work with the Services provider to maintain the ongoing list of DMS approved reasons for an SLA clock suspension. In order to qualify for an SLA suspension (hold time), one of those approved reasons must be documented in the Services provider’s NOC ticketing system. However, for Operational IMAC the approved reason must be documented in the CSAB system. A current list of approved SLA hold times for the Services provider is:

- Incorrect address provided by the Customer.
- Customer not available at time of turn-up.
- Customers being unresponsive to calls or emails.
- Site readiness requirement not fulfilled by the Customer.

The Services provider will not be held accountable for SLAs due to Force Majeure as defined in the **Attachment B, Draft Contract**.

SLAs shall apply in the event of human error, such as a change during a non-maintenance window that was thought to be safe but resulted in an outage or performance degradation.

The Services provider will not be held accountable for SLAs if the redundant MFN-3 Services Infrastructure prevents service interruption.

SLAs will not be waived for any redundant systems under MFN-3 during scheduled maintenance window (including emergency) approved by the DMS.

SLAs do not apply for any non-redundant systems under MFN-3 during scheduled maintenance windows (including emergencies) approved by DMS. However, SLAs for any issues caused due to and after the scheduled maintenance window, are not exempt. Outages, including those caused by human error which are beyond the scope of the approved maintenance change request, are not exempt.

An outage caused by poor engineering design and configuration issues is not exempt from SLA violations.

Outages caused by unpublished or unannounced software bugs in deployed equipment such as routers and firewalls are exempt from SLA violations. However, outages or performance degradation caused by published software bugs not corrected by the Services provider shall not be exempt from SLAs.

Tardy dispatch, and dispatch without required repair/diagnostic tools, expertise, and spare equipment does not exempt the Services provider from their accountability for SLA restoral of the services.

DMS will make the final determination on the Services provider compliance with SLAs.

3.1.2 Service Credits

Non E-rate Eligible Sites: DMS receives 100% of the service credits for non E-rate eligible sites.

E-rate Eligible Sites: For sites that choose Service Provider Invoice (SPI) E-rate billing:

- The Services provider shall return the discounted portion of the service credits to USAC and the non-discounted portion of the service credits to DMS.

For sites that choose Billed Entity Applicant Reimbursements (BEAR) E-rate billing: The Services provider shall return 100% of the service credits to DMS.

3.1.3 Performance Monitoring Baseline

The Services provider's final implementation of the performance monitoring service will be verified against **Attachment C, Service Level Agreements** during production go-live implementation to assure that MFN-3 performance monitoring is effective in production. Any parameters not meeting the requirements of the SLA matrix must be corrected prior to production.

3.1.4 Scrubbing Alerts

DMS and its Customers must be able to receive alerts when MFN-3 Services SLAs are not met. Even with a sophisticated suppression process there will be spurious alerts which will need to be scrubbed. DMS and the Services provider shall each be part of the scrubbing and validation process. Any SLA disputes resulting from the SLA

scrub and validation process shall be escalated to DMS and the Services provider's management for resolution.

Indicate how alerts can be suppressed under circumstances when the alert is not an operational concern and therefore would not result in an SLA violation.

Discuss the general administrative process where the teams work to scrub the data and how data is to be sifted to yield meaningful subset of alerts, when the various teams meet, and their responsibilities in the scrubbing process. Where possible, use examples of alerts (records) pulled from a production implementation of the monitoring system.

Describe the detailed process for providing SLA service credits for failing to meet service level agreements.

3.1.5 Dynamic SLAs

DMS's intention is to utilize a suite of performance monitoring systems to detect instances when any MFN-3 service is not performing per the Statement of Work requirements. Since the network itself, and the tools to manage performance, are expected to evolve and improve during the Contract term, to guarantee robust performance monitoring, service level functionality shall be redefined as needed and as it becomes possible to adopt SLAs that result in better performance to MFN end-users. Any update of SLAs or performance monitoring services will be accomplished via operational discussions with the Services provider where DMS deems it appropriate and then ratified with appropriate Contract amendments or change orders.

3.1.6 Timely Credit Determination and the Application of Credits

Timely credit determination and the application of credits are critical to DMS because there are fiscal accounting deadlines; grant terms and conditions and rules related to accounting practices. If the various fiscal deadlines are not met, there are actual monetary losses to the State of Florida. Credits shall be applied to the appropriate account within the target time window shown within **Attachment C, Service Level Agreements**.

3.1.7 Scrubbing Alerts Production Implementation

Provide information about the existence of at least one production implementation of the proposed scrubbing functionality. Indicate the size and scope of the production implementations. DMS reserves the right to view the implementation or request additional information on the implementation and may contact staff at the organization where the system is in production.

SECTION 4.0 Financial Consequences for Non-Performance

4.1 Withholding Payment or Other Remedies

4.1.1 Consequences for Non-Performance

In addition to the specific consequences explained herein, the Department reserves the right to withhold payment or implement other appropriate remedies, such as Contract termination and recovery of damages, when the Services provider has failed

to perform and/or comply with provisions of the Contract. These consequences for non-performance shall not be considered penalties.

SECTION 5.0 SLA Migration and Transition Planning (Support Services)

5.1 Migration from MFN-2 to MFN-3

These subsections cover technical, administrative, and contractual topics associated with the migration from FIRN-2, MFN-2, and any other related contracts to MFN-3. Subsections in 5.2 cover the transition between MFN-3 and the future replacement to the MFN-3 contract. The distinction between the terms migration and transition is intended to clarify that there are two distinct efforts. The Services provider shall provide a project plan that details the plan and timeline to implement all Core Services Infrastructure for readiness to transition services from MFN-2 to MFN-3.

5.1.1 MFN-3 Core Services Readiness Plan

Provide a detailed plan with milestones for readiness

Conduct design discussions with DMS on items including but not limited to the build-out of Core, Internet, Security and NMS tools suite infrastructure

Develop documentation including but not limited to:

- COOP and MFN-3 Services Infrastructure plans,
- Project/Migration plans,
- CPE Certified CPE List,
- Training guides for network, security and NMS tools,
- Reference guides for all products offered under the NMS and security tool suite,
- Product catalog,
- CSAB to vendor system integration and billing,
- SUNCOM website content,
- Staffing plans,
- Inspection plan
- Detail validation testing script plan
- NOC and SOC processes and procedures

After the contract has been executed, the Service Provider will have 180 days to be ready to begin migrating Customers to MFN-3. The Services provider will have 18 months from the MFN-3 Services Infrastructure checklist acceptance date to migrate Customers from MFN-2 to MFN-3.

A milestone for the readiness of each core service should be part of the MFN-3 Network readiness plan.

The final milestone should reflect readiness of the MFN-3 Network services to begin transitioning of sites and services from MFN-2 to MFN-3. This “Services Readiness Date” will be used by DMS as a date to be able to start transitioning MFN-2 Customers to MFN-3.

5.1.2 Migration Plan – Sites and Services

As part of the reply, provide a detailed narrative describing the Migration Plan for sites listed on the Site Inventory migrating to MFN-3. In addition, the Services provider must provide a final migration plan after Contract execution as part of the MFN-3 Services Readiness Plan.

All Project Management documents must be submitted as either a Microsoft Word 2016 (or higher) document, or Adobe PDF. The Project Management Implementation Schedule shall be submitted as a Microsoft Project document. All Project Management documents will be submitted to DMS and are subject to approval and acceptance by the Department. Any deliverables submitted but not accepted by the Department will be subject to the applicable financial consequences until the Department accepts the deliverable.

In accordance with the requirements set forth in Section 2.25 – Project Management, provide a detailed Project Management Plan and Project Schedule. The Project Management Plan is a deliverable subject to final acceptance by DMS. The Project Management Plan is the document that describes how the project is monitored, controlled, and executed. The deliverable must meet the Project Risk and Complexity Category 4 requirements of Chapter 60GG-1.002, F.A.C. Include sufficient detail to address all phases of the migration. Include detailed timelines and activities with deliverables and milestones that will be used to track progress toward the goal of implementing MyFloridaNet-3. Include the resources allocated to each activity including the names and number of hours each migration team lead will spend with each Customer. Include the proposed timeline for Customer submittal and approval of orders. Two weeks before the MFN-3 Services Infrastructure is approved for production, DMS shall refresh the current network Site Inventory to create a final MFN service Site Inventory. Place the Microsoft Project plan in the reply packet following the instructions provided in the ITN instructions Section 3.7, Contents of Reply, and **Attachment E, Reply Format** (see TAB 7).

The Services provider must account for all timelines and activities as they develop the details for the migration plan. DMS will provide accurate CSAB orders in a timely fashion, but all other Services migration tasks are the responsibility of the Services provider.

5.1.3 Migration - Staffing Resource Requirements

Staffing for the migration is critically important to the success of the project due to the large number of Customer sites represented in the Site Inventory. Place the definition of the level of staffing in Attachment H, Staffing Plan Worksheet. Provide a detailed narrative to explain the staffing resource requirements for a successful migration.

Define and provide sufficient technical project managers, general project managers, engineering teams, and any other resources needed to meet the migration timeline specified in the related SLAs.

Due to economic conditions, Customers have gone through a number of downsizing efforts since the inception of MFN. Consequently, Customers do not have adequate network engineering staff to be assigned to provide a high level of support for migration planning and implementation activities. DMS and the Customer base will not be able

to augment staff to address the migration. To ensure this is not detrimental to the process, the Services provider must provide all additional necessary resources to ensure successful migration.

Provide detail on how the Services provider will group, by name, each of the Customers with their respective migration team. The Services provider must expect to be present onsite with the Customer teams, and the reply needs to illustrate the importance of this requirement.

5.1.4 Migration - Knowledge Transfer

Provide a detailed narrative used to explain the knowledge transfer activities as defined in the migration plan. Describe the knowledge transfer processes used by the Services provider's teams as they work with the current MFN-2 service provider to gain knowledge of the specifics of the MFN-2 design and the current standard operating procedures.

5.1.5 Migration – Project Management Tasks and Related Deliverables

DMS will actively monitor the Services provider's compliance with Migration project management requirements.

Without creating the final migration plan, provide enough detail to demonstrate the Respondent understands the project management tasks that are required to migrate an Enterprise. For the specific project management tasks, and the related deliverables, describe how the tasks listed below will be provided.

5.1.6 Migration - Communication Plan

Communication Plan activities cover development and implementation of the Communication Plan. The timeline must include sufficient time for the DMS Communications Office to review and approve the various iterations of the Communications Plan. DMS requires day-to-day involvement with the Services provider in the migration planning process and actual migration activities. The Services provider will be required to spend significant time communicating the project status in various forums throughout the migration.

The Communication Plan must address these elements:

- Identify key stakeholders.
- Provide communications timely and accurately.
- Provide feedback mechanisms to ensure feedback is appropriately reviewed.
- Adjustment of the Communication Plan as necessary to improve gaps identified through the process.
- How the Services provider will proactively develop correspondence to Customers during migration and throughout the life of the contract.
- Identify the stakeholders and the amount of time needed for the various communication efforts with DMS, the Customer Chief Information Officers, and Customer management.
- Maintain a log to document all issues throughout the project; list ongoing and closed issues of the project; organize issues by type, severity, to prioritize

issues associated milestones or deadlines. Issue logs must contain Customer requests and remarks about the various problems.

- Using a bi-weekly dashboard to summarize and update the project status to upper management and Customers (their management and those responsible for the Customer's migration). The dashboard must keep participants informed without all the details provided in the meeting minutes, project schedules, and the issue log.
- Create and maintain a directory structure to be used in the Services provider's public facing website to maintain all revisions of the project management documents including issues logs and dashboards.
- Host meetings with established objectives and goals. The Respondent must provide agendas prior to the meeting with enough notice and detail for the participants to be able to prepare and decide if their participation is needed. Once a meeting is scheduled, Respondent shall not cancel meeting without prior DMS written approval.
- Provide active direction as the host of the meeting. Ensure meetings capture changes in the project schedule and action items in sufficient detail to use to update documents and related project materials.
- Ensure meeting minutes are kept at a level of detail where participants that cannot attend have access to all salient information. At a minimum this includes date, time, topics discussed, actions, background for decisions made, narrative for topics of discussion, and individuals responsible for action items.

5.1.7 Migration - Engineering Review

It is critical that a comprehensive technical engineering review take place with DMS acting as the facilitator between the current MFN-2 Services Provider and the MFN-3 Services provider. To ensure an accurate MyFloridaNet-3 Services Infrastructure, all technical aspects of the physical, logical, and technical definitions for the current MFN network must be documented by the Respondent. This documentation should be utilized in the migration planning phase with the Services provider's project managers and engineering teams. Careful consideration should be given to MFN Customers whereby critical public safety services are provided to ensure there is no impact on public safety Customers. Adequate planning and testing are critical steps to ensure that no service interruptions occur. Provide a detailed narrative on the engineering plan to migrate sites listed on the Site Inventory to MFN-3.

5.1.8 Migration - Provisioning Planning

Proper provisioning planning is the identification of all physical components and assets required to deliver each service to an MFN-3 Customer. The Services provider's project management team must address each MFN-3 Customer's provisioning needs adequately to avoid service interruption. The final migration plan developed during the MFN-3 Services Infrastructure build-out must show a separate migration project plan unique to each Customer that outlines the following:

- CPE requirements (CPE can be provided by the Services provider or by the Customer)
- Service type
- Service requirements

- Service configuration, to include all routing definitions
- Service nature, e.g., critical public safety, general use, best effort, etc.
- MFN Customer involvement capabilities, e.g., does the Customer have network engineering staff available
- Critical dates that preclude migration of service, such as Legislative Session, Public events, etc.

Without creating the final migration plan, provide enough detail to demonstrate the Respondent understands the provision planning required to migrate an Enterprise.

5.1.9 Migration - Network Operations Center

Provide a detailed narrative on the proposed plan to migrate the NOC function from the MFN-2 provider to the new MFN-3 service provider. Network Operations Center migration planning narrative is important since there will be a MyFloridaNet-2 NOC, and the Services provider's NOC providing services simultaneously.

5.1.10 Migration - Administrative Services

Provide a detailed narrative used to migrate administrative services from current contracts to the new MFN-3 service provider. The migration of Customer service, account services, and billing services are critical activities. Provide a detailed narrative of the requirements for Customer service and account team interaction. Describe how those systems will be implemented with their respective interfaces to CSAB.

5.1.11 Migration - Payment Strategy Connection-By-Connection

The Services provider must use a migration strategy utilizing a connection-by-connection payment strategy where all costs to the Services provider are paid only as each site/service migrates to MFN-3. DMS will not pay any upfront cost for MFN-3 network development.

5.1.12 Migration - Connection Testing Period with Fall Back Option

It is the Services provider’s responsibility to work with each Customer to define their disconnect date(s) and work with them to submit appropriate disconnect paperwork on MFN-2. As a site migrates to the MFN-3 network and DMS accepts in writing that a circuit has been activated successfully, there will be a fifteen (15) calendar day live testing period at no cost. During the testing period, the site can fall back to the current network (MFN-2) at no cost in the event of technical concerns preventing the site’s successful migration. If the migration is successful, the Services provider will begin billing for the new MyFloridaNet-3 connection after the fifteen (15) calendar day live testing period. If the migration is not successful and the Customer falls back to the current network connection, the live testing period restarts; the Customer will always have fifteen consecutive days to run on the MyFloridaNet-3 connection before MyFloridaNet-3 billing begins. At the Customer’s option, the Services provider will permit a site to extend their fallback window beyond the fifteen (15) calendar day interval. Customers electing to extend the fallback window assume responsibility for charges for both connections after the fifteen (15) calendar day live test period.

5.1.13 Migration - Special Construction

There shall be no special construction charges for like-for-like bandwidth and media for sites being migrated from MFN-2 to MFN-3. The Service Provider is responsible for migration of Customers from these current services at no cost. Individual Customers are responsible for special construction costs after migration to MFN-3.

5.2 Transition between MFN-3 and the Successor Contract

5.2.1 Transition Introduction

These subsections cover technical, administrative, and contractual topics associated with the transition between MFN-3 and the replacement contract for MFN-4.

5.2.2 Transition - Contract Completion

There will be a need for end of contract transition services as upon expiration or termination of the MyFloridaNet-3 contract; therefore, the Respondent will work with DMS to devise a transition plan and process to enable a smooth transition of services from MFN-3. The full transition of existing services to follow-on contract(s) is hereby explicitly made a condition of the MFN-3 service. These transition activities will be met before the MFN-3 contract is considered complete.

5.2.3 Transition - Payment Strategy Connection-By-Connection

DMS requires a transition strategy utilizing a connection-by-connection payment strategy. As sites migrate from MFN-3 to any replacement contract, DMS will continue to pay only for each site still served under the MFN-3 contract. During the transition phase, payments to the MFN-3 Respondents will decrease in number as sites migrate to the follow-on contract.

5.2.4 Transition - Overlapping Contracts

Overlapping contracts are required when transitioning from one large infrastructure to another. The transition could take several years; therefore, it must begin before the expiration of the MFN-3 contract. Sites and services are not considered an exclusive award to the MFN Services provider, nor does the MFN-3 Services provider have an exclusive right to offer network services to SUNCOM Customers. Sites and services can be migrated from the MFN-3 contract to a replacement contract(s) prior to the expiration date of the MFN-3 contract and any replacement contracts. DMS is not obligated to maintain MFN-3 contracted services for any set number of Customers or locations, but the MFN-3 Services provider is obligated to continue providing MFN-3 services regardless of the number of Customers or locations remaining on the MFN-3 network. If the MFN-3 contract is terminated before the expiration date, the transition period will begin as required by DMS.

5.2.5 Transition - Contract Terms, Conditions, and Rates

The MFN-3 provider will maintain business as usual for all MFN-3 services until there is a successful transition of all Customers to a replacement MFN infrastructure. MFN-3 contract terms, conditions, and rates will remain unchanged during the transition period.

5.2.6 Transition - New Work Orders during Transition Period

During the transition phase, new work orders will be accepted by the Services provider to provide uninterrupted services for MFN-3 Customers until the replacement contract has been fully executed, and the replacement contractor(s) are ready to accept orders. The current terms, conditions, and rate will apply to new orders. Once a replacement contract for MFN-3 has been signed, any new work orders will be reviewed by DMS and approved only if the work order cannot be satisfied by the replacement provider.

5.2.7 Transition - Expeditious Efforts during the Transition

DMS recognizes that as sites disconnect from the MFN-3 infrastructure the revenue will decrease yet the MFN-3 infrastructure will remain largely in place. DMS, the Services provider, and the replacement provider(s) will collaborate to migrate to the replacement contract as expeditiously as possible. During the development of the contract with a replacement provider, DMS will define milestones for the replacement provider to attempt to avoid sites languishing on the MFN-3 infrastructure.

5.2.8 Transition - End of Contract Transition Assistance

During the effort to transition between MFN-3 and the replacement contract, the Services provider will work with DMS and any applicable current and follow-on contractors as determined by DMS to devise a transition plan and process to enable a smooth transition between MFN-3 and the replacement contract.

As part of the end of contract transition assistance, the Services Provider will:

- Provide sufficient efforts and cooperation to ensure an orderly and efficient transition of service to the replacement contract. These efforts include taking all necessary steps, measures, and controls to ensure minimal disruption of services during the transition.
- Deliver to DMS, upon request, whether previously made available, the following:
    - Up-to-date operations guides and procedures the Services Provider follows to provide MFN-3 Services.
    - All documentation created for the purpose of supporting, operating, maintaining, upgrading, and enhancing services, including but not limited to, up-to-date operational manuals, training guides, design documents, and configurations for core and CPE.
    - Disclosure of the equipment, software, and third-party contract services required to perform MFN-3 services for DMS.
    - Databases of information, providing database dumps of ordering and billing information as needed.
- Assist DMS and the replacement provider(s) with the planning and installation of any network-to-network related connections to facilitate business continuity for the MFN-3 sites. (Generally, the replacement provider would be responsible for paying for new network connections supporting the orderly and efficient transition.)
- Answer questions related to the transition on an as-needed basis. Under MFN-3, the Services Provider must provide transition services assisting DMS and the

follow-on provider(s) when understanding these and other operational and procedural aspects of MFN-3.

- To the extent reasonable, provide such other services, functions, or responsibilities inherent or necessary to the transition of services to substantially similar services, provided that such services, functions, or responsibilities are limited to those that can be delivered with the then current Services provider's team staffing (including subcontractors if required).

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK