State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
MPLS07	1

ADDRESS CORRESPONDENCE TO ATTENTION OF:
RON PRICE
304-558-0492

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
ALL STATE AGENCIES
AND POLITICAL SUBDIVISIONS
VARIOUS LOCALES AS INDICATED
BY ORDER

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
11/21/2006				

BID OPENING DATE: 02/08/2007 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
0001	1	LS		205-18		

MULTI PROTOCOL LABEL SWITCHING (MPLS) VIRTUAL

PRIVATE NETWORK (VPN) SERVICES & ASSOCIATED SERVICES
PER THE ATTACHED SPECIFICATIONS

A MANDATORY PRE-BID SHALL BE HELD AT THE WEST VIRGINIA OFFICE OF TECHNOLOGY, ONE DAVIS SQUARE, CHARLESTON, WV ON JANUARY 5, 2007 AT 10:00 AM. EACH VENDOR MUST BE REPRESENTED PHYSICALLY AT THE PRE-BID. VENDORS ARE REQUIRED TO PRE-REGISTER AT LEAST 24 HOURS IN ADVANCE, VIA E-MAIL NOTIFICATION TO RON PRICE, AT RPRICE@WVADMIN.GOV. THE FOLLOWING INFORMATION SHOULD BE INCLUDED IN THE E-MAIL RESPONSE: FIRM, REPRESENTATIVE NAME, MAILING ADDRESS, TELEPHONE NUMBER FAX NUMBER, AND E-MAIL ADDRESS OF THE REPRESENTATIVE. FAILURE TO HAVE A REPRESENTATIVE PHYSICALLY IN ATTENDANCE AT THE PRE-BID CONFERENCE SHALL RESULT IN DISQUALIFICATION OF THE BID. NO ONE PERSON CAN REPRESENT MORE THAN ONE BIDDER.

VENDOR PREFERENCE CERTIFICATE

CERTIFICATION AND APPLICATION* IS HEREBY MADE FOR PREFERENCE IN ACCORDANCE WITH WEST VIRGINIA CODE, 5A-3-37 (DOES NOT APPLY TO CONSTRUCTION CONTRACTS).

A. APPLICATION IS MADE FOR 2.5% PREFERENCE FOR THE REASON CHECKED:

( ) BIDDER IS AN INDIVIDUAL RESIDENT VENDOR AND HAS RESIDED CONTINUOUSLY IN WEST VIRGINIA FOR FOUR

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

GENERAL TERMS & CONDITIONS
REQUEST FOR QUOTATION (RFQ) AND REQUEST FOR PROPOSAL (RFP)

1. Awards will be made in the best interest of the State of West Virginia.

2. The State may accept or reject in part, or in whole, any bid.

3. All quotations are governed by the ***West Virginia Code*** and the ***Legislative Rules*** of the Purchasing Division.

4. Prior to any award, the apparent successful vendor must be properly registered with the Purchasing Division and have paid the required $125.00 registration fee.

5. All services performed or goods delivered under State Purchase Orders/Contracts are to be continued for the term of the Purchase Order/Contract, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise available for these services or goods, this Purchase Order/Contract becomes void and of no effect after June 30.

6. Payment may only be made after the delivery and acceptance of goods or services.

7. Interest may be paid for late payment in accordance with the ***West Virginia Code.***

8. Vendor preference will be granted upon written request in accordance with the ***West Virginia Code.***

9. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

10. The Director of Purchasing may cancel any Purchase Order/Contract upon 30 days written notice to the seller.

11. The laws of the State of West Virginia and the ***Legislative Rules*** of the Purchasing Division shall govern all rights and duties under the Contract, including without limitation the validity of this Purchase Order/Contract.

12. Any reference to automatic renewal is hereby deleted. The Contract may be renewed only upon mutual written agreement of the parties.

13. **BANKRUPTCY:** In the event the vendor/contractor files for bankruptcy protection, this contract is automatically null and void, and is terminated without further order.

14. **HIPAA Business Associate Addendum -** The West Viginia State Government HIPAA Business Associate Addendum (BAA), approved by the Attorney General, and available online at the Purchasing Division's web site (**http://www.state.wv.us/admin/purchase/vrc/hipaa.htm**) is hereby made part of the agreement. Provided that, the Agency meets the definition of a Covered Entity (45 CFR §160.103) and will be disclosing Protected Health Information (45 CFR §160.103) to the vendor.

INSTRUCTIONS TO BIDDERS

1. Use the quotation forms provided by the Purchasing Division.

2. **SPECIFICATIONS:** Items offered must be in compliance with the specifications. Any deviation from the specifications must be clearly indicated by the bidder. Alternates offered by the bidder as **EQUAL** to the specifications must be clearly defined. A bidder offering an alternate should attach complete specifications and literature to the bid. The Purchasing Division may waive minor deviations to specifications.

3. Complete all sections of the quotation form.

4. Unit prices shall prevail in cases of discrepancy.

5. All quotations are considered F.O.B. destination unless alternate shipping terms are clearly identified in the quotation.

6. **BID SUBMISSION:** All quotations must be delivered by the bidder to the office listed below prior to the date and time of the bid opening. Failure of the bidder to deliver the quotations on time will result in bid disqualifications.

SIGNED BID TO:

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
MPLS07	2

ADDRESS CORRESPONDENCE TO ATTENTION OF:
RON PRICE
304-558-0492

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
ALL STATE AGENCIES
AND POLITICAL SUBDIVISIONS
VARIOUS LOCALES AS INDICATED
BY ORDER

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
11/21/2006				

BID OPENING DATE: 02/08/2007 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

(4) YEARS IMMEDIATELY PRECEDING THE DATE OF THIS CERTIFICATION; OR

( ) BIDDER IS A PARTNERSHIP, ASSOCIATION OR CORPORATION RESIDENT VENDOR AND HAS MAINTAINED ITS HEADQUARTERS OR PRINCIPAL PLACE OF BUSINESS CONTINUOUSLY I WEST VIRGINIA FOR FOUR (4) YEARS IMMEDIATELY PRECEDING THE DATE OF THIS CERTIFICATION; OR 80% OF THE OWNERSHIP INTEREST OF BIDDER IS HELD BY ANOTHER INDIVIDUAL, PARTNERSHIP, ASSOCIATION OR CORPORATION RESIDENT VENDOR WHO HAS MAINTAINED ITS HEADQUARTERS OR PRINCIPAL PLACE OF BUSINESS CONTINUOUSLY IN WEST VIRGINIA FOR FOUR (4) YEARS IMMEDIATELY PRECEDING THE DATE OF THIS CERTIFICATION; OR

( ) BIDDER IS A CORPORATION NONRESIDENT VENDOR WHICH HAS AN AFFILIATE OR SUBSIDIARY WHICH EMPLOYS A MINIMUM OF ONE HUNDRED STATE RESIDENTS AND WHICH HAS MAINTAINED ITS HEAQUARTERS OR PRINCIPAL PLACE OF BUSINESS WITHIN WEST VIRGINIA CONTINUOUSLY FOR THE FOUR (4) YEARS IMMEDIATELY PRECEDING THE DATE OF THIS CERTIFICATION.

B. APPLICATION IS MADE FOR 2.5% PREFERENCE FOR THE REASON CHECKED:

( ) BIDDER IS A RESIDENT VENDOR WHO CERTIFIES THAT, DURING THE LIFE OF THE CONTRACT, ON AVERAGE AT LEAST 75% OF THE EMPLOYEES WORKING ON THE PROJECT BEING BID ARE RESIDENTS OF WEST VIRGINIA WHO HAVE RESIDED IN THE STATE CONTINUOUSLY FOR THE TWO YEARS IMMEDIATELY PRECEDING SUBMISSION OF THIS BID;
OR
( ) BIDDER IS A NONRESIDENT VENDOR EMPLOYING A MINIMUM OF ONE HUNDRED STATE RESIDENTS OR IS A NONRESIDENT VENDOR WITH AN AFFILIATE OR SUBSIDIARY

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
MPLS07	3

ADDRESS CORRESPONDENCE TO ATTENTION OF:
RON PRICE
304-558-0492

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
ALL STATE AGENCIES
AND POLITICAL SUBDIVISIONS
VARIOUS LOCALES AS INDICATED
BY ORDER

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
11/21/2006				

BID OPENING DATE: 02/08/2007 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

WHICH MAINTAINS ITS HEADQUARTERS OR PRINCIPAL PLACE OF BUSINESS WITHIN WEST VIRGINIA EMPLOYING A MINIMUM OF ONE HUNDRED STATE RESIDENTS WHO CERTIFIES THAT, DURING THE LIFE OF THE CONTRACT, ON AVERAGE AT LEAST 75% OF THE EMPLOYEES OR BIDDERS' AFFILIATE'S OR SUBSIDIARY'S EMPLOYEES ARE RESIDENTS OF WEST VIRGINIA WHO HAVE RESIDED IN THE STATE CONTINUOUSLY FOR THE TWO YEARS IMMEDIATELY PRECEDING SUBMISSION OF THIS BID.

BIDDER UNDERSTANDS IF THE SECRETARY OF TAX & REVENUE DETERMINES THAT A BIDDER RECEIVING PREFERENCE HAS FAILED TO CONTINUE TO MEET THE REQUIREMENTS FOR SUCH PREFERENCE, THE SECRETARY MAY ORDER THE DIRECTOR OF PURCHASING TO: (A) RESCIND THE CONTRACT OR PURCHASE ORDER ISSUED; OR (B) ASSESS A PENALTY AGAINST SUCH BIDDER IN AN AMOUNT NOT TO EXCEED 5% OF THE BID AMOUNT AND THAT SUCH PENALTY WILL BE PAID TO THE CONTRACTING AGENCY OR DEDUCTED FROM ANY UNPAID BALANCE ON THE CONTRACT OR PURCHASE ORDER.

BY SUBMISSION OF THIS CERTIFICATE, BIDDER AGREES TO DISCLOSE ANY REASONABLY REQUESTED INFORMATION TO THE PURCHASING DIVISION AND AUTHORIZES THE DEPARTMENT OF TAX AND REVENUE TO DISCLOSE TO THE DIRECTOR OF PURCHASING APPROPRIATE INFORMATION VERIFYING THAT BIDDER HAS PAID THE REQUIRED BUSINESS TAXES, PROVIDED THAT SUCH INFORMATION DOES NOT CONTAIN THE AMOUNTS OF TAXES PAID NOR ANY OTHER INFORMATION DEEMED BY THE TAX COMMISSIONER TO BE CONFIDENTIAL.

UNDER PENALTY OF LAW FOR FALSE SWEARING (WEST VIRGINIA CODE 61-5-3), BIDDER HEREBY CERTIFIES THAT THIS CERTIFICATE IS TRUE AND ACCURATE IN ALL RESPECTS; AND THAT IF A CONTRACT IS ISSUED TO BIDDER AND IF ANYTHING CONTAINED WITHIN THIS CERTIFICATE CHANGES DURING THE TERM OF THE CONTRACT, BIDDER WILL NOTIFY THE PURCHASIN

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
MPLS07	4

ADDRESS CORRESPONDENCE TO ATTENTION OF:
RON PRICE
304-558-0492

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
ALL STATE AGENCIES
AND POLITICAL SUBDIVISIONS
VARIOUS LOCALES AS INDICATED
BY ORDER

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
11/21/2006				

BID OPENING DATE: 02/08/2007 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

DIVISION IN WRITING IMMEDIATELY.

BIDDER: ----------

DATE: ----------

SIGNED: ----------

TITLE: ----------

* CHECK ANY COMBINATION OF PREFERENCE CONSIDERATION(S) IN EITHER "A" OR "B", OR BOTH "A" AND "B" WHICH YOU ARE ENTITLED TO RECEIVE. YOU MAY REQUEST UP TO THE MAXIMUM 5% PREFERENCE FOR BOTH "A" AND "B".
(REV. 12/00)

NOTICE

A SIGNED BID MUST BE SUBMITTED TO:

DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
BUILDING 15
2019 WASHINGTON STREET, EAST
CHARLESTON, WV 25305-0130

THE BID SHOULD CONTAIN THIS INFORMATION ON THE FACE OF THE ENVELOPE OR THE BID MAY NOT BE CONSIDERED:

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
MPLS07	5

ADDRESS CORRESPONDENCE TO ATTENTION OF:
RON PRICE
304-558-0492

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
ALL STATE AGENCIES
AND POLITICAL SUBDIVISIONS
VARIOUS LOCALES AS INDICATED
BY ORDER

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
11/21/2006				

BID OPENING DATE: 02/08/2007 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
	SEALED BID					
	BUYER: 41					
	RFQ. NO.: MPLS07					
	BID OPENING DATE AND TIME					
	PLEASE PROVIDE A FAX NUMBER IN CASE IT IS NECESSARY TO CONTACT YOU REGARDING YOUR BID:					
	_____					
	CONTACT PERSON (PLEASE PRINT CLEARLY):					
	_____					
	****** THIS IS THE END OF RFQ MPLS07 ****** TOTAL:					_____

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
The West Virginia Office of Technology

REQUEST FOR PROPOSAL

Statewide Multi Protocol Label Switching (MPLS) Virtual Private Network (VPN) Services & Associated Services

RFP No.MPLS07 for WV-MPLS & Associated Services

Sealed Proposal Due By:

February 8, 2006, 1:30 PM ET

All available information concerning this Request for Proposal may be downloaded from the West Virginia Office of Technology. Web Site: www.WVOT.gov.

Refer ALL Inquires to: Ron Price Buyer Supervisor
Purchasing Division
2019 Washington Street, East
Charleston, WV 25305-0130
Telephone: 304-558-0492
Fax: 304-558-4115\
E-mail: @wvadmin.gov

7

Table of Contents

9

11

13

APPENDICES

Appendix A– WV Voice, Video and Data Access Types - Current State (Approximation)

Appendix B – Pricing Tables and Instructions

Appendix C – Alternative Access Offerings (Access Circuits, Wireless, IP-Trunking/Hosted Voice Services)

Appendix D –Alternative Access and IP Voice Circuits Pricing (for Options listed in Appendix C)

Appendix E – Pricing for all Vendor-provided Options

Appendix F – Vendor References

REFERENCES

Current Voice Contract (Centrex & **DAIN**) electronic at **WVOT Website:** www.wvgot.org.

Current Data 05 Contract: Electronic copy at **WVOT Website:** www.wvgot.org.

VENDOR CHECKLIST – CRITICAL REQUIREMENTS

This checklist has been provided for the convenience of the responding vendors. Vendors shall demonstrate their understanding and compliance with these "Critical RFP Requirements" by checking each Section Reference in the following table, indicating that they have responded with the information required to support the critical requirement **in their text response to the RFP.** Note: if vendors do not respond to the Critical requirements as requested, they risk significant point reductions.

Section Reference	Critical Requirement	Vendor's Acknowledgment of Compliance
3.1.3.1	MPLS Routing	
3.1.3.2	Core Network	
3.1.3.3	Logical Partitions	
3.1.3.4	VRF Management	
3.1.3.5	Layer 3 Routing	
3.1.3.6	Non-Standard Based Services	
3.1.3.7	NAT Transversal	
3.1.3.8	IPv6 Transition	
3.1.4.1	Statewide Connectivity	
3.1.5	High Availability and Reliability	
3.1.6.1	Quality of Service (QoS)	
3.1.6.2	QoS Functionality within the MPLS (PE to PE)	
3.1.7.1	Class of Service Forwarding	
3.1.7.3	FEC Classes	
3.1.11.4	QoS Methodology	
3.1.11.5	Fault Tolerance	
3.1.11.6	Traffic Rerouting	
3.1.12.3	Access Facility Types Supported	
3.1.12.6	Access Circuits Service Billing	
3.1.13.3	Signaling Protocols	
3.1.14.4	Existing Centrex and PRI Traffic	
3.1.14.5	Legacy Interoperability	
3.1.14.6	Facility Changes	
3.1.15.1	VoIP Portfolio	
3.1.15.3	Agency Intra-MPLS toll requirements	
3.1.15.5	Double-Billing Prohibition	
3.1.15.10	Highly Desired Features Response Compliance	
3.1.15.20	IP T1/PRI Trunking Generic	
3.1.15.23	QoS and DiffServ Signaling	
3.1.17.1	Access Circuit Services	
3.1.17.1.1	User Perspective/Mesh Technology	
3.1.17.2	Access Circuit Installation and Testing	
3.1.17.8	Third Party Circuits	
3.1.21.2	USAC Compliance	
3.1.21.3	Universal Services Fund	

3.2.4.1	On-Going Maintenance	
3.2.4.2	Scheduled Maintenance	
3.2.4.3	Advance Notification	
3.2.4.4	Emergency Maintenance	
3.2.5.2	Vendor's Acknowledgement of Response to Appendices	
3.2.7.2	Configuration Records	
3.2.8	Dynamic and Manual Rerouting Tracking	
3.2.9.1	Monitoring	
3.2.9.2	Service Provider's NOC	
3.2.9.3	Alarm and Alert Monitoring System Application	
3.2.9.5	Performance and Error Monitoring	
3.2.9.6	Bandwidth Utilization and Exception Monitoring	
3.2.9.10	Access to Alarm and Alert System or Application	
3.2.9.12	Alarm and Alert System or Application Training	
3.3.1	Trouble Ticketing Function	
3.3.2	Trouble Ticketing System	
3.3.4	Notification Back to WVOT	
3.3.8	Advance Outage Notification	
3.3.20	Intrusive Testing	
3.3.21	Trouble Ticketing System Reports	
3.4.1	Reporting	
3.4.2	Report on Verification of MPLS VPN Traffic Processing	
3.5.1	Service Requests (TCRs)	
3.5.4	Service Outage Escalation and Reporting Procedures	
3.5.5	Statistical Reporting	
3.5.11	Inventory	
3.6.4	Circuit Database	
3.7.1	MACD Charges	
3.7.2	Travel Costs	
3.10.1	Vendor Billing Point of Contact	
3.10.2	Billing Presentation	
3.10.3	Electronic Billing	
3.10.5	SB700 Compliance	
3.10.6	SB700 Billing Exceptions	
3.11	Billing Cycle	
3.11.2	New Service Billing	
3.12.2	Circuit ID	
3.12.4	Sample of Categorization	
3.12.8	Penalties	
3.12.9	Records	
3.12.10	Audit Documentation	
3.12.11	TCR Requirements	
3.13.1	Credits for Billing Errors	
3.13.2	Credit Resolution	

3.16.1.1	Inclusive Costs	
3.16.1.2	Implementation Team	
3.16.1.3	Implementation Plan	
3.16.1.5	Project Team Requirements	
3.16.1.10	Project Manager's Responsibilities	
3.16.1.13	Implementation Team's Equipment Requirements	
3.16.1.14	Implementation Team's VPN Access	
3.16.1.15	Project Plan	
3.16.2.1	Design Plan	
3.16.5.1	Prior Project Experience	
3.16.5.2	Customer References	
3.16.6.4	Subcontractor Performance	
3.16.7.1	All Sites	
3.16.7.2	Liquidated Damages for Missed Timeline	
3.16.9.1	Cut-Over Methodology	
3.16.9.2	Cut-Over Backout	
3.16.9.3	Cut-Over Change Management	
3.16.9.4	Cut-Over Test Plan	
3.16.10.2	Default Acceptance	
3.16.10.4	Acceptance Billing	
3.16.12.1	Disentanglement Approach and Process	
3.16.12.2	Cooperation and Information	
3.16.12.3	Continued Service	
3.17.1	Maintenance Requirements	
3.17.3.1	Guarantees	
3.17.3.2	Exclusions	
3.17.3.3	MPLS VPN (CE to CE) Network Minimum Service Standards Table	
3.17.3.4	Backbone Availability Requirements	
3.17.3.6	Backbone Availability Remedy	
3.17.3.7	Backbone Latency Guarantee	
3.17.3.9	Backbone Jitter	
3.17.3.12	Backbone Packet Delivery	
3.17.3.15	Outage Notification	
3.17.3.20	SLA Service Guarantees and Remedies	
3.17.4.2	Access Circuit Availability	
3.18.5.2.1	VoIP Jitter SLA Performance	
3.18.5.3	Network Latency Service Level Agreement	
3.18.5.4	Network Packet Delivery Service Level Agreement	
3.18.5.5	Network Availability Service Level Agreement	
3.19.2	Inclusive Pricing	
3.19.5.1	Rates	
3.19.5.2	Competitive Market	

NOTE: Vendors MUST NOT include any cost in the sections referenced above. All costs associated with bid responses MUST appear in Appendices B, D and E, and be provided separately from the technical responses to this RFP.

Revised: 10/16/2006

REQUEST FOR PROPOSAL
West Virginia Office of Technology

PART 1 GENERAL INFORMATION/TERMS AND CONDITIONS

1.1 **Purpose:**

The Acquisition and Contract Administration Section of the Purchasing Division, hereinafter referred to as "State", is soliciting proposals for the Department of Administration, West Virginia Office of Technology (WVOT), hereinafter referred to as "Agency", to replace the WVOT's aging statewide, private OC-3, DS-3 backbone that now serves state Agencies, higher education, county and municipal government, schools, libraries, and law enforcement, with an aggregated ATM, Frame Relay, DSL and a separate Voice/DAIN/Centrex network. As the business needs of the State have changed over the life of the existing network; it has become evident that the State needs to move toward a vendor-provisioned network that is more robust, flexible, redundant and capable of combining the needs of video, voice, and data onto one platform, in an effort to reduce the State's overall communications cost. The Voice/DAIN contract will stay in effect, with the expectation that migration from the DAIN to IP Trunking and Hosted IP Voice Solutions will take place over the life of the MPLS contract and subsequent renewals.

1.2 **Project:**

It is the State's desire to select an experienced Prime Vendor that will result in the State of West Virginia having a Multi-Protocol Label Switching (MPLS) network which will be utilized by all non-exempt, and most exempt, State Agencies and may be leveraged by County and WV Municipalities. The Core MPLS Network cost is to be bid at a zero dollar cost over the life of the contract. The cost of said MPLS core described in detail herein this RFP document will be distributed over the thousands of voice and data connections in a "postage stamp" pricing approach. The pricing of said voice and data connections are to be based solely on the Access Type, Port Size and Class of Service. The winning Prime Vendor will be evaluated based on experience in deploying like size, or greater, MPLS Networks and their response to the requirements of this RFP. Vendors should demonstrate the ability to meet the State of West Virginia's specific needs and the ability to smoothly transition from our current Voice/DAIN & DATA 05 Contract Network environment(s) in the time allocated to complete the transition.(Response to the technical portion of the RFP).

The Vendor will be evaluated based upon their technical ability, experience, and the overall value of their products and services in the technical evaluation, (70%) and the overall costs (30%) of said products and services based on three (3) intelligently projected cost evaluation scenarios, in accordance with the Department of Purchasing's guidelines.

The Office of Technology realizes that many of our State's counterparts' procurements of MPLS Networks resulted in a consortium of Vendors working together under a Prime Vendor to deliver the best value solution. That approach is certainly viable here in West Virginia, however it is not required and in any case the Prime Vendor will be solely responsible for the delivery and maintenance of the contract receivables. The Office of Technology is utilizing and

leveraging several of our State counterpart's RFPs, as well as our subscription to Gartner, to develop this RFP with strong, enforceable, Service Level Agreements.

1.3 **RFP Format:**
This RFP has four parts. "Part 1" contains general information/terms and conditions, "Part 2" describes the background and working environment of the project, "Part 3" is a statement of the specifications for the services requested pursuant to this RFP, contractual requirements, and special terms/conditions and "Part 4" explains the required format of the Bidder's response to the RFP, the evaluation criteria the State will use in evaluating the proposals received, and how the evaluation will be conducted.

1.4 **Inquiries:**
Additional information inquiries regarding specifications of this RFP must be submitted in writing to the State Buyer with the exception of questions regarding proposal submission which may be oral. The deadline for written inquiries is identified in the Schedule of Events, Section 1.16. All inquiries of specification clarification must be addressed to:

Ron Price Buyer Supervisor
Purchasing Division
2019 Washington Street, East
P.O. Box 50130
Charleston, WV 25305-0130
Fax: (304) 558-4115

Absolutely NO contact shall be made by the vendor with any member of the evaluation committee. Violation may result in rejection of the bid. The State Buyer named above is the sole contact for any and all inquiries after this RFP has been released.

1.5 **Vendor Registration:**
Vendors participating in this process should complete and file a Vendor Registration and Disclosure Statement (Form WV-1) and remit the registration fee. Vendor is not required to be a registered vendor in order to submit a proposal, but the successful bidder must register and pay the fee prior to the award of an actual purchase order/contract.

1.6 **Oral Statements and Commitments:**
Vendor must clearly understand that any verbal representations made or assumed to be made during any oral discussions held between Vendor's representatives and any State personnel is not binding. Only the information issued in writing and added to the Request for Proposal specifications file by an official written addendum are binding.

1.7 **Economy of Preparation:**
Proposals should be prepared simply and economically, providing a straightforward, concise description of Vendor's abilities to satisfy the requirements of the RFP. Emphasis should be placed on completeness and clarity of content.

1.8 **Labeling of RFP Sections:**
The sections within this RFP contain instructions governing how the Vendor's proposal is to be arranged, submitted and to identify the material to be included therein.

1.8.1 **Critical and Optional Requirements:**
The sections in part 3 and 4, annotated as "CRITICAL," describe the specifications which are the foundation of this procurement. The vendor is expected to provide a description of their solution, in detail. The vendor will be evaluated based on their responses to these requirements, so it is not in the best interests of the vendors to respond with a simple "yes" or "no" response to these sections.

All pricing for critical specifications are to be included in the base price such as listed in Appendix B. Pricing for optional specifications other than those in Appendix B should be included on Appendix E. Appendices C and D are for the vendor to provide different access circuits that may not have been covered in the RFP. Appendix C is for the vendor to provide a description of the access circuits noting the relevant page and section references. Appendix D is a pricing sheet showing the cost of these additional access circuits. Again, the vendor should provide the relevant page and section references for ease of understanding. Appendix C should be included with the technical submission while Appendix D should be included with the cost submission. No pricing for any offering, whether critical or optional, shall appear in the body of the vendor's response to this RFP. All pricing is to be presented in the noted cost appendices (B, D, and E).

Vendors are hereby put on notice that if they should choose to take exception to one of the critical specifications, it is at their own peril, and may negatively impact their score and the Evaluation Team's determinations and findings. Only those exceptions submitted in writing, as part of the Vendor's Proposal, shall be considered exceptions. All mandatory language, regardless of designation, contained in this RFP shall constitute binding contractual obligations upon incorporation into a final agreement with the Selected Vendor, subject to any exceptions also incorporated into the final, executed Agreement, and the successful negotiated SLA(s).

1.8.2 Contract Terms and Conditions:
This Request for Proposal contains all the contractual terms and conditions under which the State of West Virginia will enter into a contract.

1.8.3 Informational Sections:
All information specifications do not require a response from the vendor. They are intended to aid the vendor in structuring an effective proposal capable of meeting the needs of the issuing agency.

1.9 **Proposal Format and Submission:**
1.9.1 Vendors must complete a response to all critical specifications in order to be considered. Each proposal should be formatted as per the outline in Part 4 of this RFP. No other arrangement or distribution of the proposal information may be made by the bidder. Failure on the part of the bidder to respond to specific requirements detailed in the RFP may be basis for disqualification of the proposal. The State reserves the right to waive any informality in the proposal format and minor irregularities.

1.9.2 State law requires that the original technical and cost proposal be submitted to the Purchasing Division. All proposals must be submitted to the Purchasing Division prior to the date and time stipulated in the RFP as the opening date. All bids will be date and time stamped to verify official time and date of receipt.

1.9.3 Vendors mailing proposals should allow sufficient time for mail delivery to ensure timely arrival. In accordance with State Code 5A-3-11, the Purchasing Division cannot waive or excuse late receipt of a proposal which is delayed and late for any reason. Any proposal received after the bid opening date and time will be immediately disqualified in accordance with State law and the administrative rules and regulations.

Submit:
One original technical and cost
Plus seven (7) convenience copies to:

Purchasing Division
2019 Washington Street, East
P.O. Box 50130
Charleston, WV 25305-0130

The outside of the envelope or package(s) should be clearly marked:
Buyer: _41_____
Req#: _MLPS07_____
Opening Date: _02/08/07_____
Opening Time: 1:30 P. M.

1.9.4. **Best Value Purchasing Standard Format**
All Requests for Proposals should follow the standard format defined by the Purchasing Division. This format addresses required areas and enables the agency to modify the background and scope of work to meet its needs.

1.9.4.1 **Evaluation Criteria:** All evaluation criteria must be clearly defined in the specifications section and based on a 100 point total score. Based on a 100 point total, cost shall represent a minimum of 30 of the 100 total points in the criteria.

1.9.4.2 **Proposal Format and Content:** Proposals shall be requested and received in two distinct parts: Technical and Cost. The cost portion shall be sealed in a separate envelope and will not be opened initially. **NO PRICING FOR ANY OFFERING, WHETHER CRITICAL OR OPTIONAL SHALL APPEAR IN THE BODY OF THE VENDOR'S RESPONSE TO THIS RFP. ALL PRICING MUST BE PRESENTED IN THE NOTED COST APPENDICES.**

1.9.4.3 **Technical Bid Opening:** The Purchasing Division will open only the technical proposals on the date and time specified in the Request for Proposal. The Purchasing Division representative will read aloud the names of those who responded to the solicitation. The Purchasing Division Buyer will confirm that the original packages contain a separately sealed cost proposal prior to providing the courtesy copies to the agency to begin the evaluation process.

1.9.4.4 **Technical Evaluation:** The pre-selected, approved evaluation committee will review the technical proposals, deduct appropriate points for deficiencies and make a final written consensus recommendation to the Purchasing Division Buyer. If the Buyer approves the committee's recommendation, the technical evaluation will be forwarded to an internal review committee within the Purchasing Division.

1.9.4.5 **Cost Bid Opening:** Upon approval of the technical evaluation from the internal review committee, the Purchasing Division shall schedule a time and date to publicly open and read aloud the cost proposals. The agency and the vendors shall be notified of this date.

1.9.4.6 **Cost Evaluation and Resident Vendor Preference:** The evaluation committee will review the cost proposals, assign appropriate points and make a final consensus recommendation to the Purchasing Division. In accordance with West Virginia State Code §5A-3-37, the Purchasing Division will make the determination of the Resident Vendor Preference, if applicable. Resident Vendor Preference provides an opportunity for qualifying vendors to request (at the time of bid) preference for their residency status. Such preference is an evaluation method only and will be applied only to the cost bid in accordance with the West Virginia State Code. A certificate of application is used to request this preference. Generally, a West Virginia vendor may be eligible for two 2.5% preferences in the evaluation process.

1.9.4.7 **Contract Approval and Award:** After the cost proposals have been opened, the evaluation committee completes its review and prepares the final evaluation making its recommendation for contract award based on the highest scoring vendor. The final evaluation is submitted to the Purchasing Division buyer. Once approved by the buyer, the final evaluation must be reviewed and approved by the Purchasing Division internal review committee. The contract is prepared and signed in the Purchasing Division, forwarded to the Attorney General's Office for approval as to form, encumbered and mailed to the appropriate parties.

1.10 **Rejection of Proposals:**
The State shall select the best value solution according to the evaluation criteria. However, the State reserves the right to accept or reject any or all proposals, in part or in whole at its discretion. The State reserves the right to withdraw this RFP at any time and for any reason. Submission of, or receipt by the State of proposals confers no rights upon the bidder nor obligates the State in any manner.

A contract based on this RFP and the Vendor's proposal, may or may not be awarded. Any contract resulting in an award from this RFP is not valid until properly approved and executed by the Purchasing Division and approved as to form by the Attorney General.

1.11 **Incurring Costs:**
The State and any of its employees or officers shall not be held liable for any expenses incurred by any bidder responding to this RFP for expenses to prepare, deliver the proposal, or to attend any mandatory pre-bid meeting or oral presentations.

1.12 **Addenda:**
If it becomes necessary to revise any part of this RFP, an official written addendum will be issued by the State to all bidders of record.

1.13 **Independent Price Determination:**
A proposal will not be considered for award if the price in the proposal was not arrived at independently without collusion, consultation, communication, or agreement as to any matter relating to prices with any competitor unless the proposal is submitted as a joint venture.

1.14 **Price Quotations:**
The price(s) quoted in the bidder's proposal will not be subject to any increase and will be considered firm for the life of the contract unless specific provisions have been provided for adjustment in the original contract.

1.15 **Public Record:**

1.15.1 **Submissions are Public Record**
All documents submitted to the State Purchasing Division related to purchase orders/contracts are considered public records. All bids, proposals, or offers submitted by bidders shall become public information and are available for inspection during normal official business hours in the Purchasing Division Records and Distribution center after the award is complete and documents have been microfilmed.

1.15.2 **Written Release of Information**
All public information may be released with or without a Freedom of Information request, however, only a written request will be acted upon with duplications fees paid in advance. Duplication fees shall apply to all requests for copies of any document. Currently the fees are $0.50/page, or a minimum of $10.00 per request which ever is greater.

1.15.3 **Risk of Disclosure**
The only exemptions to disclosure of information are listed in West Virginia Code §29B-1-4. Primarily, only trade secrets as submitted by a bidder are the only exemption to public disclosure. The submission of any information to the State by a vendor puts the risk of disclosure on the vendor. The State will make a reasonable effort not to disclose information that is within the guidelines of §29B-1-4 and is properly labeled "proprietary information not for public disclosure". The State does not guarantee non-disclosure of any information to the public.

1.16 Schedule of Events:

Release of the RFP	11/20/06
Vendor's Written Questions Submission Deadline.	12/27/06
Mandatory Pre-bid Conference	01/05/07*
Addendum Issued	01/12/07
Bid Opening Date	02/08/07

*NOTE: The vendor conference must be 30 days from the release of the RFP for E-rate compliance.

1.17 **Mandatory Pre-bid Conference:**
A mandatory pre-bid conference shall be conducted on the date specified above at 10:00a.m. Said conference will be hosted by the West Virginia Office of Technology, One Davis Square, Charleston, West Virginia. The State intends to offer remote attendance, via conference call, to accommodate vendor representatives who may be honoring pre-existing obligations elsewhere. **However, each vendor must have a representative physically present for the pre-bid.** Vendor(s) are required to pre-register, at least 24 hours in advance, via e-mail notification to Ron Price, at rprice@wvadmin.gov. The following information should be included in the email response: firm, representative name, mailing address, telephone number, fax number and email address of representative. All interested bidders are required to participate in this

meeting. Failure to participate in the mandatory pre-bid conference shall automatically result in disqualification. No one person can represent more than one vendor. **The Mandatory Pre-bid Conference is the opportunity for the Vendor to ask questions, voice concerns, and offer suggestions. Each Vendor should read the entire RFP and come to the conference with a full understanding of what the State hopes to achieve with the RFP, or the questions necessary to obtain clarification.**

1.18 **Affidavit:**
West Virginia State Code §5A-3-10a requires that all bidders submit an affidavit regarding any debt owed to the State. The affidavit must be signed and submitted prior to award. It is preferred that the affidavit be submitted with the proposal.

1.19 **General Terms and Conditions:**

By signing and submitting their proposal, the successful Vendor agrees to be bound by all the terms contained in this RFP.

1.19.1 **Conflict of Interest:**
Vendor affirms that it, its officers or members or employees presently have no interest and shall not acquire any interest, direct or indirect which would conflict or compromise in any manner or degree with the performance or its services hereunder. The Vendor further covenants that in the performance of the contract, the Vendor shall periodically inquire of its officers, members and employees concerning such interests. Any such interests discovered shall be promptly presented in detail to the Agency.

1.19.2 **Prohibition against Gratuities:**
Vendor warrants that it has not employed any company or person other than a bona fide employee working solely for the vendor or a company regularly employed as its marketing agent to solicit or secure the contract and that it has not paid or agreed to pay any company or person any fee, commission, percentage, brokerage fee, gifts or any other consideration contingent upon or resulting from the award of the contract.

For breach or violation of this warranty, the State shall have the right to annul this contract without liability at its discretion, and/or to pursue any other remedies available under this contract or by law.

1.19.3 **Certifications Related to Lobbying:**
Vendor certifies that no federal appropriated funds have been paid or will be paid, by or on behalf of the company or an employee thereof, to any person for purposes of influencing or attempting to influence an officer or employee of any Federal entity, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment or modification of any Federal contract, grant, loan, or cooperative agreement.

If any funds other than federally appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee or any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in

connection with this Federal contract, grant, loan, or cooperative agreement, the Vendor shall complete and submit a disclosure form to report the lobbying.

Vendor agrees that this language of certification shall be included in the award documents for all sub-awards at all tiers (including subcontracts, sub-grants, and contracts under grants, loans, and cooperative agreements) and that all sub-recipients shall certify and disclose accordingly. This certification is a material representation of fact upon which reliance was placed when this contract was made and entered into.

1.19.4 **Vendor Relationship:**
The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by the parties to this contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents.

Vendor shall be responsible for selecting, supervising and compensating any and all individuals employed pursuant to the terms of this RFP and resulting contract. Neither the Vendor nor any employees or contractors of the vendor shall be deemed to be employees of the State for any purposes whatsoever.

Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension or other deferred compensation plans, including but not limited to Workers' Compensation and Social Security obligations, and licensing fees, etc. and the filing of all necessary documents, forms and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including but not limited to the foregoing payments, withholdings, contributions, taxes, social security taxes and employer income tax returns.

The Vendor shall not assign, convey, transfer or delegate any of its responsibilities and obligations under this contract to any person, corporation, partnership, association or entity without expressed written consent of the Agency.

1.19.5 **Indemnification:**
The Vendor agrees to indemnify, defend and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person or firm performing or supplying services, materials or supplies in connection with the performance of the contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use or disposition of any data used under the contract in a manner not authorized by the contract, or by Federal or State statutes or regulations; (3) Any failure of the Vendor, its officers, employees or subcontractors to observe State and Federal laws, including but not limited to labor and wage laws.

1.19.6 **Contract Provisions:**
After the successful Vendor is selected, a formal contract document will be executed between the State and the Vendor. In addition, the RFP and the Vendor's response will be included as

part of the contract by reference. The order of precedence is the contract, the RFP and the Vendor's proposal in response to the RFP.

1.19.7 **Governing Law:**
This contract shall be governed by the laws of the State of West Virginia. The Vendor further agrees to comply with the Civil Rights Act of 1964 and all other applicable laws (Federal, State or Local Government) regulations.

1.19.8 **Compliance with Laws and Regulations:**
The vendor shall procure all necessary permits and licenses to comply with all applicable laws, Federal, State or municipal, along with all regulations, and ordinances of any regulating body.

The Vendor shall pay any applicable sales, use, or personal property taxes arising out of this contract and the transactions contemplated thereby. Any other taxes levied upon this contract, the transaction, or the equipment, or services delivered pursuant here to shall be borne by the contractor. It is clearly understood that the State of West Virginia is exempt from any taxes regarding performance of the scope of work of this contract.

1.19.9 **Subcontracts/Joint Ventures:**
The Vendor is solely responsible for all work performed under the contract and shall assume prime contractor responsibility for all services offered and products to be delivered under the terms of this contract. The State will consider the Vendor to be the sole point of contact with regard to all contractual matters. The Vendor may, with the prior written consent of the State, enter into written subcontracts for performance of work under this contract; however, the vendor is totally responsible for payment of all subcontractors.

1.19.10 **Term of Contract & Renewals:**

CONTRACT TERMS
The contract that results from this RFP will remain in effect through June 30, 2009, with an option to renew for three (3) additional two (2) year periods.

This contract will not be a split award. The Sole winning Vendor may sub-contract within the proper guidelines determined by the State of West Virginia's Purchasing regulations, but the Prime Vendor shall be responsible for all criteria deliverables, SLA commitments etc..

The successful vendor must sign the attached WV-96 or applicable AG/WVOT Purchasing approved alternative form prior to award. All vendors should sign and include the WV-96 form with their proposal.

To the extent permissible by law, the vendor shall extend to the State the lowest rates and charges for all services provided in response to this Request for Proposal that it offers to any other customer similarly situated with respect to volume of service.

Describe in detail how the vendor plans to meet or exceed the aforementioned.

1.19.11 **Non-Appropriation of Funds:**
If the Agency is not allotted funds in any succeeding fiscal year for the continued use of the

service covered by this contract by the West Virginia Legislature, the Agency may terminate the contract at the end of the affected current fiscal period without further charge or penalty. The Agency shall give the vendor written notice of such non-allocation of funds as soon as possible after the Agency receives notice. No penalty shall accrue to the Agency in the event this provision is exercised.

1.19.12 **Contract Termination:**
The State may terminate any contract resulting from this RFP immediately at any time the Vendor fails to carry out its responsibilities or to make substantial progress under the terms of this RFP and resulting contract. The State shall provide the Vendor with advance notice of performance conditions which are endangering the contract's continuation. If after such notice the Vendor fails to remedy the conditions contained in the notice, within the time period contained in the notice, the State shall issue the Vendor an order to cease and desist any and all work immediately. The State shall be obligated only for services rendered and accepted prior to the date of the notice of termination.

The contract may also be terminated upon mutual agreement of the parties with thirty (30) days prior notice.

1.19.13 **Changes:**
If changes to the original contract become necessary, a formal contract change order will be negotiated by the State. The State recognizes that MPLS Networks routinely offer new access types and services to the Network Core. The State reserves the right to leverage these network enhancements and incorporate them into the contract, as they become available. These new features, services and access types connected to the MPLS Core will be considered routine technology refresh to this contract. **For all other changes to services NOT connected to the MPLS Core, a standard Change Order must be approved prior to utilizing these new services.** WVOT and the Vendor will address changes to the terms and conditions, costs of work included under the contract. An approved contract change order is defined as one approved by the Purchasing Division and approved as to form by the West Virginia's Attorney General's Office, encumbered and placed in the U.S. Mail prior to the effective date of the amendment. An approved contract change order is required whenever the change affects the payment provision and/or scope of the work. Such changes may be necessitated by new and amended Federal and State regulations and requirements.

As soon as possible after receipt of a written change request from the State, but in no event more than thirty (30) days thereafter, the Vendor shall determine if there is an impact on price with the change re-quested and provide the Agency a written statement identifying any price impact on the contract or to state that there is no impact. In the event that price will be impacted by the change, the Vendor shall, provide a description of the price increase or decrease involved in implementing the requested change.
NO CHANGE SHALL BE IMPLEMENTED BY THE VENDOR UNTIL SUCH TIME AS THE VENDOR RECEIVES AN APPROVED WRITTEN CHANGE ORDER.

The successful vendor shall participate in the E-Rate program. The vendor shall register with the Schools and Library Division of the Universal Service Administrative Company (USAC) and get a SPIN (service provider) number. Vendor must register with the USAC each year of the contract term. Vendor must remain in good standing with the USAC. Any pre-discounted E-Rate pricing will be billed to the end-sure, as dictated by the WVOT.

Describe in detail how the vendor plans to meet or exceed the aforementioned.

1.19.14 **Invoices, Progress Payments, & Retainage:**
The Vendor shall submit invoices, in arrears, to the Agency at the address on the face of the purchase order labeled "Invoice To" pursuant to the terms of the contract. Progress payments may be made at the option of the Agency on the basis of percentage of work completed if so defined in the final contract. Any provision for progress payments must also include language for a minimum 10% retainage until the final deliverable is accepted.

If progress payments are permitted, Vendor is required to identify points in the work plan at which compensation would be appropriate. Progress reports must be submitted to Agency with the invoice detailing progress completed or any deliverables identified. Payment will be made only upon approval of acceptable progress or deliverables as documented in the Vendor's report. Invoices may not be submitted more than once monthly and State law forbids payment of invoices prior to receipt of services.

1.19.15 **Liquidated Damages:** According to West Virginia State Code §5A-3-4(8), Vendor agrees that liquidated damages shall be imposed at the rate of $1,500 per day for failure to provide (deliverables, meet miles stones identified to keep the project on target, or failure to meet specified deadlines) This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue to any other additional remedy to which the State or Agency may have legal cause for action including further damages against the Vendor.

1.19.16 **Record Retention (Access & Confidentiality):**
Vendor shall comply with all applicable Federal and State of West Virginia rules and regulations, and requirements governing the maintenance of documentation to verify any cost of services or commodities rendered under this contract by Vendor. The Vendor shall maintain such records a minimum of five (5) years and make available all records to Agency personnel at Vendor's location during normal business hours upon written request by Agency within 10 days after receipt of the request.

Vendor shall have access to private and confidential data maintained by Agency to the extent required for Vendor to carry out the duties and responsibilities defined in this contract. Vendor agrees to maintain confidentiality and security of the data made available and shall indemnify and hold harmless the State and Agency against any and all claims brought by any party attributed to actions of breach of confidentiality by the Vendor, subcontractors, or individuals permitted access by Vendor.

PART 2 - OPERATING ENVIRONMENT

2.1 **Location:**

Agency's central site is located at One Davis Square, Charleston, West Virginia. West Virginia Office of Technology (WVOT) has the statutory responsibility to provide technology leadership for most State of West Virginia entities, including selection and adoption of Information Technology policy and standards and governance for expenditure of funds for Information Technology products and services. Every Executive Branch department, agency, board, bureau, commission, and authority that is subject to WVOT's jurisdiction will be required to participate in the final contract awarded under this RFP unless substantial costs can be avoided by other means of transport or a justifiable benefit can be demonstrated to the WVOT to purchase outside the awarded contract. All other State governmental entities including, but not limited to, exempt Agencies, the Judicial Branch, the Legislative Branch, the Higher Education System of West Virginia, as well as counties, and municipalities may voluntarily participate. It is anticipated that, at a minimum, the K-12 and Libraries, the Judicial and certain Higher Education entities will participate, and a factor of their Access circuits has been included in the costing scenarios for Access Circuits and Lines.

2.2 **Background:**

The West Virginia Office of Technology (WVOT) intends to replace its aging OC-3, DS-3, Centrex/DAIN and ATM/ Frame Relay (FR) network, and with time, its Centrex/DAIN contract, with a modern statewide MPLS VPN (Multi-Protocol Label Switching Virtual Private Network), for use by WVOT and WVOT customers; including state agencies and state, county, and municipal units of government, the Higher Education System of West Virginia, as well as schools and libraries. The planned MPLS VPN should enable WVOT customers to enjoy economical and reliable network access, regardless of location, and to enforce post-911 security requirements and privacy regulations. Implementation of new network technology should help agencies limit future cost growth for the network services needed to support mission-critical business requirements. The planned MPLS VPN will provide for data and video in its initial deployment, to include video conferencing, distance learning and telemedicine needs. WVOT is seeking an MPLS VPN design that will also support the deployment of Voice over IP (VoIP), specifically VoIP Trunking to CPE, "Hosted IP Centrex", (See IP Centrex/Hosted IP Voice Services, Section 3.1.15) to begin approximately three to six months after the initial deployment of the MPLS VPN.

Today, the State of West Virginia operates and maintains statewide networks for data, video and voice transmission. The current network is primarily based on mature ATM & Frame Relay (FR) technology, back-hauled and connected on linear non-redundant OC-3's and DS-3's and a separate DAIN Voice Network. This requires many individual circuits from all parts of the state to be back-hauled to Charleston, and/or Clarksburg/Morgantown, to connect with the rest of the State's network and the Internet. The State's Video Conferencing needs vary greatly and are often Agency-specific. The current ISP, WVNET, allocates bandwidth on the OC-3's and DS-3's as well as offering Video Bridging services. The voice network consists of point-to-point circuits, aggregated PRI's and Centrex Lines, and utilizes the OC-3 and DS-3 backbone, but as well as a public switched telephone network. Recently, business and security requirements have changed significantly, and new, cost-effective network technology has become available.

Over the last few years, agency business requirements for bandwidth have steadily increased because of the addition of new mission-critical business applications that utilize the network, and because of the proliferation of useful IP-based protocols that these applications use. The WVOT anticipates this growth rate to continue increasing exponentially as the State embraces 21st. Century technological initiatives including, but not limited to; E-government, E-education, virtual classrooms/distance learning and Telemedicine for the West Virginia Health Network.

Agencies are experiencing a dramatic increase in requirements for secure communications, including use of virtual private circuits, encryption, authentication, and intrusion detection. Most of these new security and privacy requirements, such as the Health Information Portability and Accountability Act (HIPAA), the Criminal Justice Information System (CJIS), or Graham-Leach-Bliley; arise from the need to satisfy Federal legislation and regulations, but some arise indirectly from the need for secure communications with State business associates, such as financial institutions, health care providers, and insurance companies which are also directly impacted by these Federal requirements.

Newer, reliable, economical, and more flexible core network technology, MPLS, has become widely available, promising better service to agency users. Additionally, less costly and more flexible network access technology such as DSL and 802.11x wireless access have become widely available. Agency demand for these technologies is strong. The need for more flexible "Hosted IP Centrex", and IP Trunking to IP based CPE/PBX's etc is also growing at a rapid rate. The Prime vendor will be required to provide these services at fixed prices throughout the State of WV regardless of ILEC, LATA or geographic density.

The planned MPLS VPN will serve the Agencies' business requirements for more bandwidth for business-critical applications, provide the foundation for secure data, video, and voice communications, provide a more reliable and more flexible core network, and, in many cases, provide network access that is far more economical than that presently available, especially for smaller government offices.

WVOT has gained practical MPLS VPN insight through recent reviews of successful Federal, State and Municipal as well as Private Sector MPLS VPN procurements or installations. The WVOT has also consulted Gartner Group, to whom which we are a subscriber, and they have confirmed our findings. The reviews were conducted to demonstrate the advantages and practicality of MPLS technology now available. Insight gained indicates that the redundant core topology of the planned MPLS VPN should alleviate the need to back-haul most network communications to Charleston, and/or Clarksburg/Morgantown, and should provide higher reliability through the ability to re-route around failed network nodes. MPLS technology allows the use of Classes of Service that should facilitate rationing and prioritizing bandwidth to best serve mission-critical applications.

The MPLS VPN solution planned for West Virginia will allow for reliable, high-bandwidth connections to all State, County, and Municipal Agencies, regardless of their geographical location. Enabling quality, high-speed network access for State Agencies located in underserved areas, particularly outside the metro Charleston, and/or the Clarksburg/Morgantown areas, is a high priority. The new MPLS VPN core network will also support the delivery of mobile solutions to mobile workers such as:

- Public Safety workers and police officers needing real-time access to Motor Vehicle Registration, Drivers' License, and other information.

- The Department of Health & Human Resources (DHHR) staff performing on-site visits and using mobile technology to chart the progress of child placements.

- The Department of Natural Resources staff working throughout State Parks and preserves.

The design of the planned MPLS VPN will provide for toll-free statewide dial-up access to enable all home or regional office workers, even those without DSL or cable modems, to securely access the MPLS VPN core network. Secure virtual private circuits will connect the worker's computer to the new State network. This will allow each worker to perform secure transactions, to safely receive, edit, and transmit documents, and to remotely access essential business applications.

Certain technical features of MPLS technology, including full-mesh topology, provide the ability to establish and, as required, self-manage or contract the management of new Private Virtual Circuits (PVCs) quickly, and have the ability to manage traffic by Class of Service (CoS). Agency IT personnel will be able to classify traffic and manage bandwidth themselves or contract this from the winning MPLS Vendor or alternate systems Integrator as their Agency's specific applications dictate. This will provide WVOT with the ability to provide better network services to WVOT customers and to limit future cost of planned growth surrounding DR and business continuity issues. WVOT is committed to spending no more on the planned MPLS VPN, associated Access Circuits, and other related services, than it spends now for the existing OC-3, DS-3, ATM/Frame Relay-based network. In fact, WVOT expects that consolidation on a single managed network topology and careful selection of Access Circuits will allow for a significant spending reduction.

This Request for Proposals (RFP), as well as accompanying Appendixes & electronic links to Attachments and Exhibits, outlines and details the plan for the contemplated MPLS VPN and related services to be quoted by prospective Service Providers. WVOT will welcome proposals from each prospective Vendor that is interested in offering a realistic, complete, and economical design for the planned MPLS VPN, with the expectation that the design can be implemented well within the intended schedule described in this RFP. Proposals that offer even shorter MPLS VRF/VPN/PVC implementation timeframes will be preferred. The WVOT has stipulated that the successful Vendor must have (4) positive like-size MPLS deployments and should be committed to maintaining the stated MPLS core for the next 7 to 10 years.

PART 3 PROCUREMENT SPECIFICATIONS

3.1 MPLS VPN Design Requirements:

The WVOT vision is an enterprise model that will foster a streamlined deployment of network components, leveraging all of the State's resources and reducing inefficiencies. MPLS is the procurement of a new enterprise communication platform under a Best Value approach. West Virginia's communication requirements span two areas: a routed component and a component integrating video, voice and other services requiring a constant traffic rate. Moving forward on the second component requires industry expertise to define integration options for the State's current routed and non-routed infrastructures.

In providing more efficient network services, State agencies will have the potential of sharing access rather than buying individual connections. WVOT **should have** the ability to capture utilization by agency. Benefits of implementing this project include reduction of communications costs incurred, eliminating duplication of effort, robust connectivity and improved security -all within an improved cost avoidance environment. Once implemented, the new technical and administrative infrastructures will meet the growing needs of the State's agencies. The WVOT MPLS initiative will deliver a statewide infrastructure providing both technical and business solutions to the State of West Virginia and its customers.

MPLS IMPLEMENTATION TIMELINE							
CENTREX/DAIN ISC51007							
	VoIP IMPLEMENTATION						
DATA05							
MPLS VPN							
3RD QTR 2007	4TH QTR 2007	1ST QTR 2008	2ND QTR 2008	3RD QTR 2008	4TH QTR 2008	1ST QTR 2009	---------- →

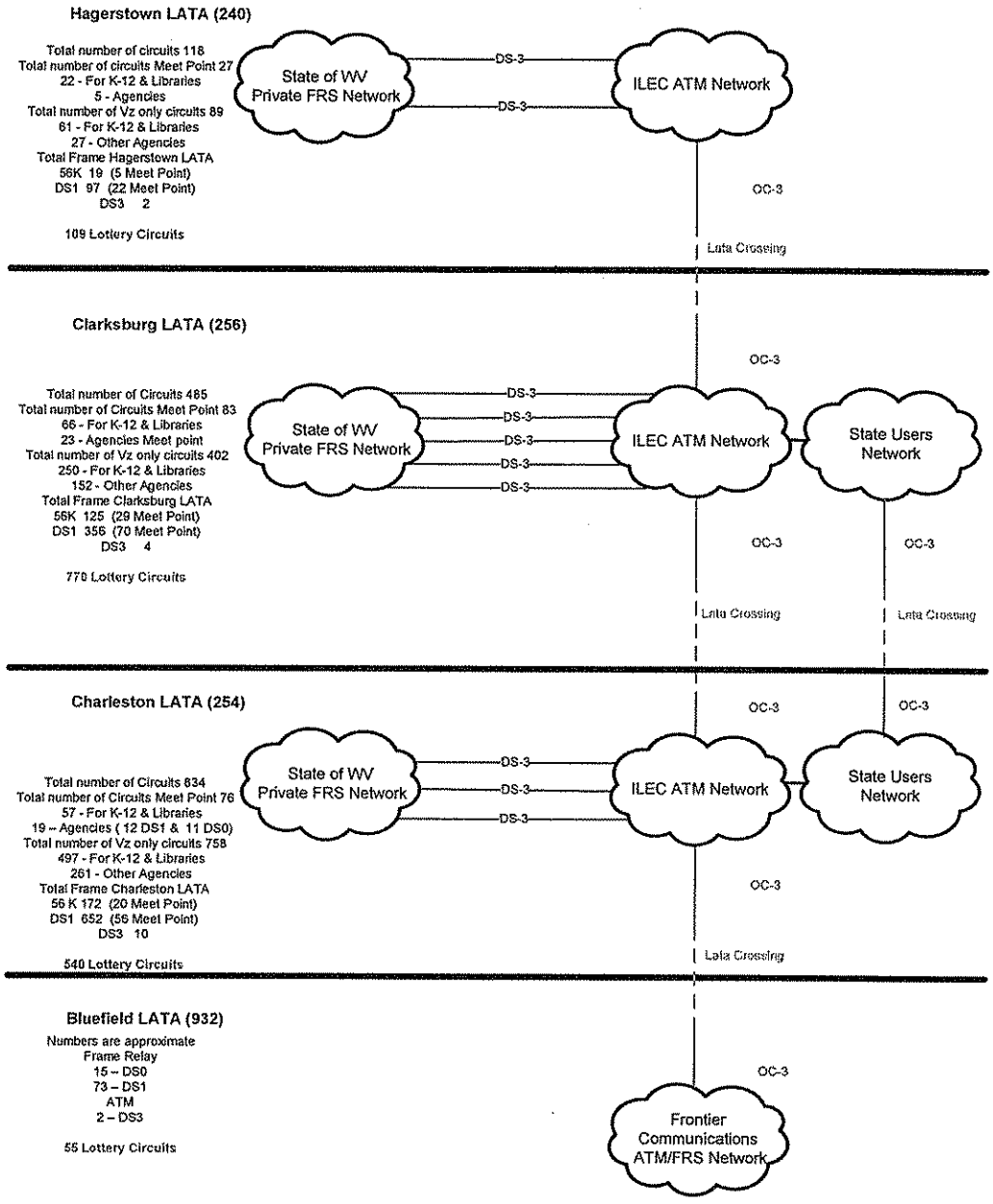
The preceding timeline is based on a February 2007 anticipated award date.

3.1.1 Current Network

The State's wide area network is comprised of an IP-based network and an SNA network. This network is used for wide area connectivity to agency locations, to the State's central data center and for Internet connectivity.

The State purchases its current Frame Relay service statewide at speeds of 56Kbs to 45Mbs. There are approximately 1800 frame relay circuits statewide. All Frame Relay circuits are backhauled to the State's backbone hubs located in Clarksburg/Morgantown and Charleston. The central core of the IP network is located in Charleston and Clarksburg/Morgantown at central data centers and all locations are served and managed from these central hubs.

The following is a breakdown by LATA of approximate existing Data 05 Contract Circuits:

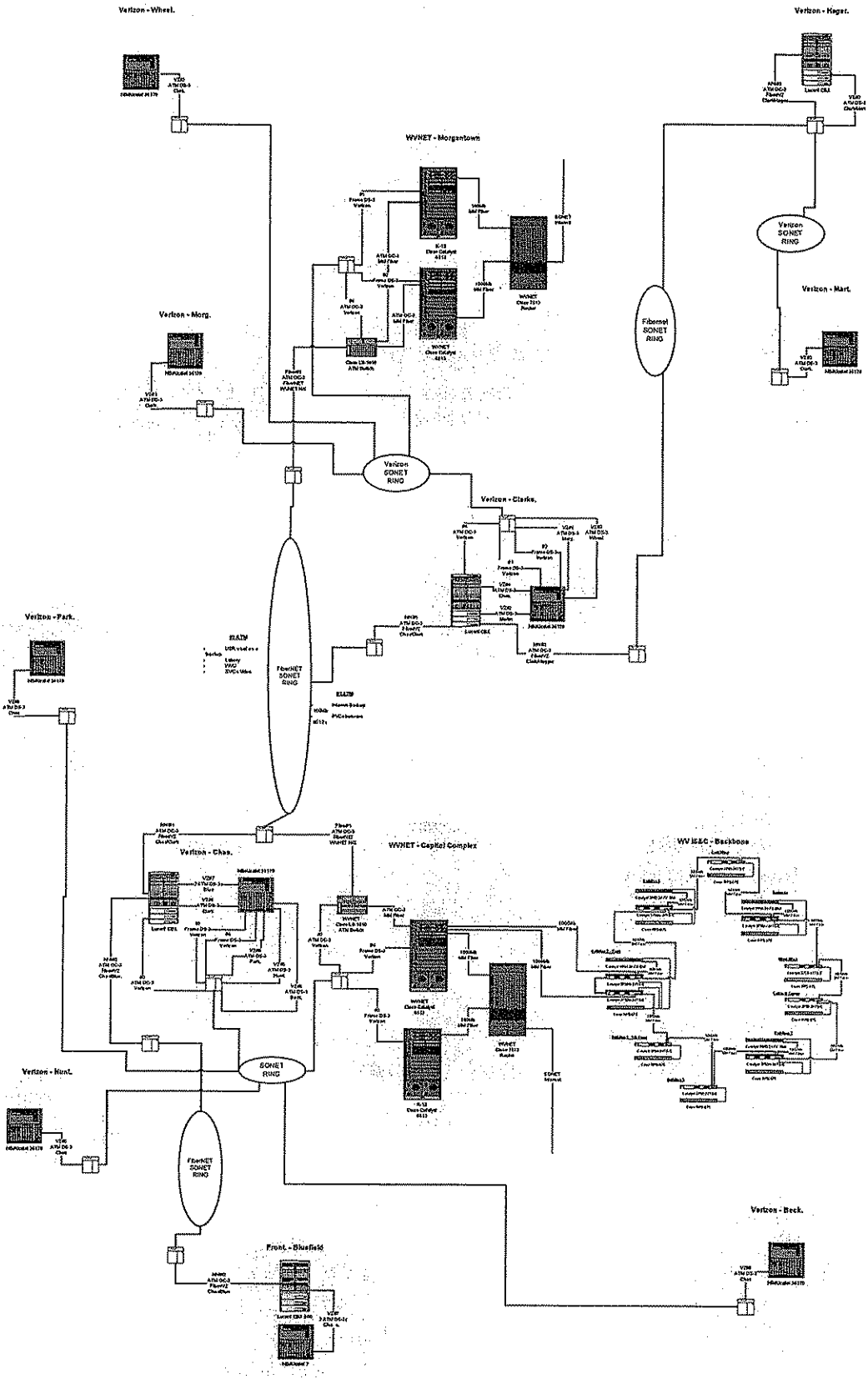


33

The Circuit quantities provided below are an intelligent estimate of what will be cut over year one from 6/30/07 to 6/30/09, although the bulk of data circuits will be cut over by 6/30/08. We are uncertain as to the quantity of Ethernet facilities and Host IP Voice Services/IPTrunks that will be added or cutover.

TYPE OF CIRCUIT	QTY	LATA240	LATA256	LATA254	LATA932
PRI – Voice 23B+D/24B	130	25	35	60	10
Transport ADSL	175	40	55	60	20
Transport SDSL	50	10	15	20	5
T-1 Clear Channel	10	2	3	3	2
FR T-1 768cir burst to full T-1	1500	350	375	580	195
DS-0 FR 56K 28Kbps min cir	250	50	75	85	40
DS-0 Clear Channel	10	2	3	3	2
Centrex	7000	1165	1600	3600	635
Centrex with Voicemail	5000	700	1100	2900	300
Switched Ethernet 10 Meg	0	0	0	0	0
Switched Ethernet 10 Meg redundant local loop	0	0	0	0	0
Switched OC-3	0	0	0	0	0
Switched OC-3 redundant local loop/true Sonnet ring	0	0	0	0	0
Switched Ethernet 1 Gigabit	0	0	0	0	0
Switched Ethernet 1 Gigabit redundant local loop					

The following roughly depicts the existing State of West Virginia Network Backbone. It does not depict the various types and speeds of access to the Network.


Verizon - Wheel.
Verizon - Hager.
WVNET - Morgantown
Verizon SONET RING
Verizon - Mart.
Verizon - Morg.
Fibernet SONET RING
Verizon SONET RING
Verizon - Clarks.
Verizon - Park.
FiberNET SONET RING
Verizon - Chas.
WVNET - Capitol Complex
WV EE/C - Backbone
SONET RING
Verizon - Hunt.
FiberNET SONET RING
Verizon - Beck.
Front. - Bluefield

The SNA network serves locations throughout West Virginia. The network provides access to the central data center mainframe computers and has approximately 62 SNA controllers with 2 to 4 printers hanging from each, and 5 peer-to-peer connections. All of the SNA traffic is encapsulated in IP packets, so there is no reason to make special SNA provisions.

The State also operates an interactive video network to provide distance learning, telemedicine, and other programs and services. The West Virginia Statewide video conferencing network uses interactive H.320 video conferencing systems connecting over the existing backbone depicted on page 26. WVNET the State's current ISP and Network management Entity provides the video bridging for most State applications.

3.1.2 Envisioned Solution and Management Framework:

The WVOT is pursuing a new communications service that will give a logical transition from where WVOT is today, to an MPLS Private IP infrastructure. It is the WVOT's long-term goal to move to a common Private IP-based network. This new infrastructure will greatly assist West Virginia in the transition toward making government products and services available instantly, twenty-four hours a day, seven days a week, and to establish a common service delivery platform for the entire enterprise.

With a managed MPLS Core infrastructure and additional managed options and related services, the WVOT will be able to redirect technical personnel towards better integrating network services into the business process, quality assurance, and maintaining appropriate security. MPLS offers a simplified service-delivery methodology, instead of competing technologies and duplicative infrastructures.

3.1.2.1 The State desires the responding vendors provide the WVOT with their vision as to how deployment of a "next generation" network, such as the requested MPLS and associated services RFP, may have economic development and other infrastructure-based advantages that may benefit West Virginia's citizens and businesses. Per the specifications noted in this RFP, this network will be used by the State of West Virginia, its counties and municipalities.

3.1.3 MPLS VPN

Core Functionality:

The WVOT requires that Multi-Protocol Label Switching (MPLS) be a core technology of the proposed network. Vendor should describe their MPLS VPN network in enough detail for WVOT to evaluate the characteristics of the Vendor's network. Should include the following:

3.1.3.1 **[Critical]** MPLS Routing: WVOT requires a core network that supports the Multi-Protocol Label Switching routing protocol. Confirm Vendor's compliance with this critical and describe the approach.

3.1.3.2 **[Critical]** Core Network: Vendor should describe, in detail, the following:

- Core/backbone with a drawing including any aggregation services.
- Interconnections between aggregation services in different areas.
- Access circuit options.
- Location of Point of Presence (POP) that will serve this network.
- Class of switches in the POPs.
- Capacity of Access Circuits within the Vendor's network.

3.1.3.3 **[Critical]** Logical Partitions: WVOT requires the ability to establish Logical Partitions of the enterprise facility that will be defined as dedicated networks for specific agencies. Confirm Vendor's compliance with this critical requirement and describe the approach for creating agency-specific "pipes" or Logical Partitions, within the common physical enterprise network, providing logical segregation with similar level of security as that of "private" networks built upon Layer 2 Private Virtual Circuits ("PVC"). NOTE: The State recognizes that, in some instances, a physical separation may be employed to accommodate the requirements.

3.1.3.4 **[Critical]** VRF Management: WVOT requires the capability to scale up to fifteen private, individual networks/VPNs/VRFs, per location, on the same access circuit. Confirm Vendor's compliance with this critical and describe the strategy for routing between the VPNs and managing the large number of VPN Routing and Forwarding (VRF) tables that such scalability would require.

3.1.3.5 **[Critical]** Layer 3 Routing: WVOT requires that the Vendor provide a scalable Layer 3 routed backbone not requiring a full PVC mesh for optimal routing. Confirm Vendor's compliance with this critical requirement and detail how the network will provide a scalable Layer 3 routed backbone to include underlying technology.

3.1.3.6 **[Critical]** Non-Standard Based Services: WVOT requires that the provisioning of services and related options will be handled by the Service Provider resulting in a standard, routed, IP only enterprise environment. Describe and explicitly identify all non-standards-based services to be used to provide MPLS VPN services.

Enterprise Network Addressing:

3.1.3.7 **[Critical]** NAT Traversal: WVOT requires support for agencies attaching to the State's WAN that use private network addresses as specified in RFC 1918 (Network Address Translation). Some additional engineering may be required to support multimedia delivery to certain sites. Confirm Vendor's compliance with this critical requirement and demonstrate how Vendor's MPLS VPN core network will address duplicate NATed private address spaces within the enterprise network.

3.1.3.8 **[Critical]** IPv6 Transition: The current State network uses an IPv4 network address scheme. Even though WVOT does not currently have a timeline for this transition, the Service Provider should work with current IPv4 network address scheme. The vendor shall propose a strategy and design for adopting and deploying IPv6 in an incremental, dispersed cost efficient manner, while providing direct interoperability between IPv6 and IPv4 systems. The vendor should have the capability to transport IPv6.0, and clearly state the date by which compliance with this critical requirement will be attained. NOTE: The State does not have a strong preference for how the vendor transports our IPv6 traffic.

3.1.4 Connectivity

3.1.4.1 **[Critical]** Statewide Connectivity: WVOT requires communications with multiple locations in the state to conduct its business. The MPLS VPN core network should provide for the connectivity needs of all currently existing State of West Virginia sites. Types of acceptable access are listed, but not limited to, those provided in Pricing Appendix B, of this RFP. Appendix B lists access types, port sizes, and classes of service which will be used for pricing evaluation. Vendors may propose alternative access types which should be listed in Appendix C, and priced separately in Appendix D. Confirm Vendor's compliance with this critical requirement. The State has included connectivity/transport access options that are likely to be utilized in the course of this contract in Appendix B. The vendor is required to provide the Access circuit types listed in appendix B when requested, within 60 days of said request, provided there are facilities for the request. The Vendor may be requested to extend facilities to new facilities within 120 days of request, or the State will maintain the option of procuring facilities from a third party or other means from the said new location back to the closest or most economic Vendor facility presence.

3.1.4.2 Future Statewide Connectivity: Beyond replacing the current network WVOT desires to ensure that the most cost effective access solutions are used for future connectivity to the MPLS VPN network. Future needs may include:

- New service addresses
- Field workers
- Temporary offices

These sites will exist in rural as well as metro areas. The Service Provider should be prepared to connect these sites in a postage stamp pricing manner. (e.g. all access types of the same type, port size and Class of Service are required to be the same across the State of WV). Vendors are encouraged to offer ideas and options reaching "outside the box" to ensure accessibility to State services. Responses should include a strategy to address these concerns.

Note: Vendors are hereby put on notice that no special consideration or access to State-owned communication towers or right-of-ways is being provided under this Procurement.

3.1.5 High Availability

[Critical] High Availability and Reliability: WVOT requires that MPLS VPN core network have high Availability (as specified in the SLA) to properly support the wide range of mission-critical applications. Define the strategy and architecture for providing high Availability within the Service Providers core network to include distinguishing features and capabilities, for proposed services.

3.1.6 Quality of Service (QoS)

3.1.6.1 **[Critical]** Quality of Service: WVOT should be able to assure agencies that critical applications receive SLA contracted resources across the network, despite varying network traffic loads - hence the need for enterprise QoS. A minimum of four (4) QoS options are required, however the State desires the vendor provide five (5) QoS options (per section 3.1.7.4.)

3.1.6.2 **[Critical]** QoS Functionality within the MPLS (PE to PE): WVOT requires end-to-end IP QoS features to preferentially handle traffic as one of the network's fundamental design philosophies to accomplish the task of managing resources within the core network. The network should be able to prioritize traffic by tagging packets in order to utilize multiple queues for voice, video and other mission critical applications and to segregate such traffic from other traffic types that are more delay-tolerant. Confirm Vendor's compliance with this critical requirement **and** describe the approach.

3.1.6.2.1 QoS End to End (CE to CE): The WVOT strongly desires a list of options by location/circuit for QoS End to End Customer Premise to Customer Premise. WVOT realizes the vendor may have difficulty pricing said offerings, due to differences in customer premise routers. NOTE: The State of West Virginia has standardized on Cisco routers. WVOT also recognizes that the vendor should manage the customer premise router. If possible, the State would like an option, by circuit type, port size and various Class of Service(s) (Best Effort to Real-Time) and number of VRFs, where the vendor supplies, manages and maintains the customer premise router. Associated pricing should be by access drop. Therefore, if the cost for a 10Mb Fast Ethernet circuit at one location, with one (1) VRF and two (2) Classes of Service, such as Best Effort and Real Time (or other vendor-offered traffic classes), the price would be $X. Additionally, the same agency has four (4) sites, with identical parameters, and another site, serving as the main site, with a 100Mb circuit, four (4) VRFs, and the same two (2) Classes of Service offered at the remote sites, with a cost of $Y. Based on these examples the State could assume that the price is four (4) times $X, plus $Y. NOTE: The vendor may wish to provide a table similar to the pricing charts provided for said managed QoS Customer Premise to Customer Premise, by access drop. **NOTE: Any vendor-included table should appear in this section for the technical portion, with any associated costs appearing in the same table format, including the pricing, in the Cost Portion of this RFP.**

3.1.6.2.2 If the vendor will support management of the existing State-owned customer premise routers, configured as a CE to enable QoS, Customer Premise to Customer Premise, vendor should describe their ability to support of said scenario. **NOTE: Any vendor-provided solution should appear in this section for the technical portion, with any associated costs included with a reference by section number, in the Cost Portion of this RFP.**

3.1.6.2.3 If the vendor does not support management of existing State routers, configured as CE, then vendor should describe their approach in this section, to working with the WVOT, or appropriate entity, to configure the existing CPE. **NOTE: Any vendor-provided solution should appear in this section for the technical portion, with any associated costs included with a reference by section number, in the Cost Portion of this RFP.**

3.1.6.2.4 If neither scenario, as described in 3.1.6.2.1 and 3.1.6.2.2, apply to the vendor's offered solution, the vendor should state how the WVOT and associated MPLS customers will be able to achieve Customer Premise to Customer Premise QoS. **NOTE: Any vendor-provided solution should appear in this section for the**

technical portion, with any associated costs included with a reference by section number, in the Cost Portion of this RFP.

3.1.6.2.5 Non-standard QoS Services: Describe any QoS functionality that is unique to the Vendor's MPLS VPN network that is not based on industry standards.

3.1.7 Class of Service Forwarding (CoS)

3.1.7.1 **[Critical]** Class of Service Forwarding: As deployed within MPLS VPN core network, MPLS Class of Service forwarding should be able to transport different types of traffic based on traffic filters, input interface, either DSCP or CoS values, MPLS labels, or any IP traffic pattern. Confirm Vendor's compliance with this critical requirement and define how the Vendor's MPLS VPN network transports different types of traffic.

3.1.7.2 Forwarding Parameter: Describe support for the ability to accept forwarding parameters from IP QoS and forward traffic based on those parameters.

3.1.7.3 **[Critical]** FEC Classes: A minimum of four (4) Forwarding Equivalence Classes (FEC), are required, ranging from "Best Effort" to "Real Time." The WVOT desires that the vendor provide five (5) FEC Classes of Service (see section 3.1.7.4). Confirm Vendor's compliance with this critical requirement and describe the Vendor's FEC classes.

3.1.7.4 Class of Service Table: Based on the following example Class of Service table, Describe Vendor's FEC classes in relation to the following table.

Example Class of Service Table

Class of Service	**Description**	**Technical Provisions**	**Applications**	Common Protocols
Teleworker	Best efforts connectivity for home office, wireless, or dial-in users at remote sites.	Latency, Bandwidth, Packet Delivery. Does not include Access Circuit.	Basic applications for teleworkers and travelers including e-mail, web browsing, Citrix, SSH, remote file access, FTP with dial-up, wireless, or DSL access.	**IP, SMTP, IMAP4, POP3, MAPI, HTTP, HTTP IPSec, Novell Protocols, LDAP, SOAP S, FTP, SSH,**
Standard Or "Best Effort"	Performance appropriate to most office and remote workers	Latency, Bandwidth, Packet Delivery. Includes Access Circuit, C.E. Router, and other CPE.	E-mail, web browsing, FTP, basic client-server transactions, VPN, SSH, Citrix, remote file shares, personal desktop streaming media including Real, WMA, QuickTime	**IP, SMTP, IMAP4, POP3, MAPI, HTTP, HTTPS, FTP, SSH, IPSec, SNA, Novell Protocols, LDAP, SOAP**
	Performance appropriate to time-critical	Latency, Bandwidth, Packet Delivery. Includes Access	Business critical applications, PeopleSoft	**IP, SMTP, IMAP4, POP3, MAPI, HT HTTPS, FTP, IPSec,**

Enhanced	applications including transaction processing	Circuit, C.E. Router, and other CPE.	transactions, client server	**SSH, SNA, Novell Protocols, LDAP, SOAP TP,**
Premium	Performance to support real-time voice and video with provisions for control of Latency and Jitter	Latency, Bandwidth, Packet Delivery, Jitter. Covers Access Circuit, including C.E. Router and other CPE.	Video conferencing, streaming video, interactive video	**To Enhanced, adds H.320 converted to IP, H.323, SIP, RTP, RTCP, RTSP**
Real-Time		**Latency, Bandwidth, Packet Delivery, Jitter. Covers Access Circuit, including C.E. Router and other CPE.**	**Voice, IP telephony**	**To Premium, adds MGCP, H.248/Megaco, G.711, G.726 (40 Kb), G.723.1, G.729, SCCP (Skinny)**

3.1.7.5 Adding FEC Classes: WVOT desires the Service Provider to be able to support additional FEC classes in the future. Describe the process for adding additional classes as necessary.

3.1.8 Bandwidth

3.1.8.1 Uniform Bandwidth Availability: WVOT strongly desires that the MPLS VPN network should ensure that bandwidth is provided uniformly across the Service Provider's core in order to provide predictable packet delivery. Describe Vendor's strategy for guaranteeing bandwidth across the MPLS VPN core network.

3.1.8.2 Rapid bandwidth increases are highly desirable. WVOT desires the capability of obtaining increases in bandwidth within a short timeframe. Beyond the logical service of altering CIR values, describe the technical features of the proposed MPLS VPN that will provide for the bandwidth of specific Service Addresses to be increased within a few days. For example: The Service Provider could participate with WVOT and agency staff working to anticipate where additional bandwidth needs will develop. The Service Provider could install high capacity Access Circuits and offer a reduction in monthly fees for unused capacity. Vendor should state if bandwidth on demand is not offered.

3.1.9 Bandwidth Reservation

WVOT strongly desires the ability to provide WVOT Customers with additional capacity on an Access Circuit as necessary to accommodate increases in traffic, such as a videoconference, or other special requirements. Describe Vendor's approach for providing Bandwidth Reservation.

3.1.10 Burst Capacity

WVOT strongly desires that circuits should be appropriately sized to provide the most cost effective transport based on the business needs of the agencies. However, occasional bursty traffic should be accommodated. Describe Vendor's strategy for supplying and managing burst capacity on a circuit.

3.1.11 Traffic Engineering

3.1.11.1 Vendor should describe their method of measuring and monitoring service levels on an end to end basis (CE to CE).

3.1.11.3 Capacity Management: WVOT strongly desires a methodology for capacity management and responsiveness. Define Vendor's methodology, timelines and any tools proposed.

3.1.11.4 **[Critical]** QoS Methodology: WVOT requires a standards-based QoS or DiffServ aware Traffic Engineering ('TE") mechanism when making forwarding decisions for passing traffic through tunnels. Describe the methodology for QoS or DiffServ TE signaling.

3.1.11.5 **[Critical]** Fault-Tolerance: WVOT requires fault-tolerance in the core as well as case-by-case on the access circuit, such as might be provided by backup tunnels. Describe Vendor's approach to fault-tolerance.

3.1.11.6 **[Critical]** Traffic Rerouting: WVOT requires the capability to automatically reroute traffic in the event transport troubles are detected. Describe the procedures to be used to initiate automatic rerouting. Include any manual procedures. Describe rerouting actions; explain which transport facility has priority over others and who can in practice initiate manual rerouting of the MPLS VPN. Discuss WVOT's role in this area including how WVOT is notified when rerouting occurs, what change procedures should be followed in the event WVOT initiates a request for change, and follow up procedures once a reroute has occurred.

3.1.11.7 Emergency Traffic Rerouting Notification: WVOT desires prompt notification when rerouting occurs in the MPLS VPN core network; especially, if the rerouting directs WVOT traffic to an alternate POP. Describe the proposed tools or procedures for this.

3.1.12 Data

3.1.12.1 **Direct Layer 2 Transport:** The State of West Virginia desires an explanation of Vendor's Layer 2 and Layer 3 transport offerings in the MPLS core.

3.1.12.2 Layer 2 Frames Transports: WVOT desires that Vendor's solution deliver Layer 2 frames. Define how Vendor's solution delivers Layer 2 frames.

3.1.12.3 **[Critical]** Access Facility Types Supported: WVOT requires that Vendor support all Access Facility types listed in Appendix A which include, but are not limited to: transport DSL, transport ADSL, Frame Relay Circuits, clear channel transport circuits (F1), DS3, OC3, 10MB Fast Ethernet, 100MB Fast Ethernet, and 1GB Fast Ethernet. Vendor's response should confirm that these facility connections to the MPLS network are supported.

3.1.12.4 IPSec VPN Services: While IPSec VPN services are not a part of this MPLS procurement, the MPLS VPN will be required to function with IPSec VPN services as a fully integrated enterprise service offering. WVOT IPSec VPN solutions will need to be integrated within the enterprise communications offering. Describe Vendor's approach to prioritizing encrypted traffic.

3.1.12.5 SNA and Legacy Protocol Support: In addition to standard IP-based routing protocols such as BGP, EIGRP, WVOT requires that the Service Provider support protocols such as SNA. Confirm Vendor's compliance with this critical requirement and describe the approach and list the network protocols that will be supported in the proposed solution, including both routed and non-routed protocols. All of the State's SNA traffic is encapsulated in IP.

3.1.12.6 **[Critical]** The State of WV cannot accept double billing therefore it is required that the MPLS Vendor provide the new MPLS Access Circuits Service at no charge until the existing facilities are removed and billing has ceased. This period is a "not to exceed" 30-day period, i.e., billing can commence 30 days after installation. **Exceptions to this are K-12 and the Library Commission which are subject to E-Rate and will be converted last. They will require ninety (90) days without double-billing.**

3.1.13 Multimedia:

3.1.13.1 The planned MPLS VPN should accommodate the secure connectivity, transmission and convergence of voice, video, and data application traffic. Within the State's enterprise, IP Multicast is the desired method to intelligently replicate a data stream, only where such replication is necessary, conserving bandwidth and resources.

3.1.13.2 It is highly desirable that the State of WV contract with a vendor who facilitates peering arrangements with multiple in-state broadband ISPs. This desirable is in an effort to promote West Virginia-based ISP services and facilitate efficient and optimal utilization of commodity Internet bandwidth into and out of the state. This will help facilitate applications such as multi-cast. Describe vendor's approach to accomplish the above.

3.1.13.2.1 The WVOT desires that bidding vendors explain, in detail, their IP Video Bridging Services offered, and if such services are proposed, please respond with the price of said optional services in Appendix E, and only Appendix E. **Please clearly label the pricing and the option, with reference to this associated section, 3.1.13.2.1.**

3.1.13.3 **[Critical]** Signaling Protocols: WVOT requires that the proposed solution support signaling protocols including but not limited to the most currently approved versions of Session Initiation Protocol (SIP), H.323, Media Gateway Control Protocol (MGCP), and H.248/Megaco. SIP and H.323 use RTP to transport real-time transmission of multimedia data over network services. Real Time Protocol (RTP), Real Time Control Protocol (RTCP), and Real Time Streaming Protocol (RTSP) transport and manage the real-time transmission of multimedia data over network services. List the protocols Vendor intends to support. List and describe any nonstandard protocols or extensions.

3.1.13.4 Multicast Update: The State of West Virginia desires vendors to explain how charges will be applied for Multicasting, and if they offer multicasting, the State desires a listing of all multicasting options. The multicasting option charges should be presented in the appropriate pricing appendix.

3.1.13.5 Compatibility: It is highly desirable that the Vendor's solution propose IP Multicast which supports compatible across multiple vendor platforms. Any State agency should be able to connect to the network and participate in IP Multicast network-wide, regardless of CPE manufacturer, as long as the CPE complies with standard IP Multicast protocols. The network should have the capability to run all standard IP Multicast and related generic protocols. Detail how Vendor's proposed solution can support standard IP multicast protocols.

3.1.14 Voice

3.1.14.1 CODECs: In order to support WVOT's plan to add VoIP services in the near future the network solution should support standard CODECs. Standard compression/decompression (CODEC) techniques, with their respective mean opinion scores (MOS), include, but are not limited to: G.711 – 4.3 MOS, G.729 – 4.0 MOS. What CODECs does the Vendor's solution support? Responses should include descriptions of any non-standard protocols or extensions.

3.1.14.2 Voice over IP: WVOT desires to allow telephony and other audio signals to be transported over the same network as regular data traffic. Describe how the proposed solution supports the eventual migration to a VoIP solution. Include information regarding the support of both a network based or WVOT premise based solutions and the risks and benefits of each approach. The State and WVOT recognize that we are responsible for preparing the premise infrastructure to support Voice and Video. With the understanding that the State has the obligation to ensure that the existing customer-premise LAN is designed to accommodate the desired volume of IP voice traffic needed to adequately support the number of simultaneous calls required; please describe:

A: What process the vendor offers to audit the existing customer-premise LAN,

B: What process the vendor will utilize to adequately size and specify the type of access facility from the MPLS CE to the customer-premise LAN,

C: What process the vendor will use to recommend the Class of Service on said recommended access type and size.

If possible, please provide an hourly rate for the auditing of the existing CPE LAN environments to ensure proper functionality for the above-stated utilization, following the noted instructions below.

NOTE: Any vendor-provided response to these specifications should appear in this section for the technical portion, with any associated costs included with a reference by section number, in the Cost Portion of this RFP.

3.1.14.2.1 The WVOT desires that the vendor describe how they will ensure voice quality IP phone to IP phone, in both a fully managed scenario, and in a scenario where the vendor has audited the existing CPE LAN and found it to be acceptable for the end users' intended IP voice volume. (e.g. How does the vendor measure and monitor voice quality from IP phone to IP phone in the aforementioned scenarios.)

3.1.14.3 Details of our current phone system are located in the Centrex and DAIN contracts on the WVOT website. The Vendor's solution should accommodate the existing analog TDM Voice (Centrex), PRI and existing T-1's provided by Verizon as it is converted to either a hosted IP based Voice solution or IP trunks on the new MPLS over a period of years. Describe in detail how the vendor proposes to allow the existing Voice Network to interact, (make toll free calls) without diminishing any other services during this multi year transition period. It is highly desirable that the State of West Virginia not increase toll costs during the transition from existing voice (DAIN) network to the new IP-based service on the MPLS.

3.1.14.4 **[Critical]** It is a requirement that the MPLS network be able to carry the State's existing Centrex and PRI traffic once they are converted to Hosted IP Services and IP Trunking on the MPLS. State your compliance with this Critical requirement.

3.1.14.5 **[Critical]** It is required that the new IP-based Voice product locations of any flavor be able to call the legacy Centrex and PRI/DAIN locations without toll charges or any other ancillary charges until all desired Centrex and PRI's are converted to IP based voice solutions on the MPLS. It is acceptable for the vendor to charge for calls to non-DAIN locations. Please describe here how the vendor would charge for such calls to non-DAIN locations if there is a charge, and include any charges (cost per minute) for such calls to non-DAIN locations in Appendix E. (i.e. The State of WV does not want to incur any more charges for in-State LD than we do today on the DAIN to DAIN calls.)

3.1.14.6 **[Critical]** The State shall not incur double facility charges during this transition, therefore the winning vendor will need to install and test the IP voice circuits, and any hosted IP Voice Service, at no charge, until the Legacy Centrex and or other legacy voice service regardless of the legacy service, vendor, and location within the State of WV can be disconnected and billing for said legacy service is terminated with a limitation of 30 days after the new IP voice service is installed. **Exceptions to this thirty (30) day limit are all E-Rate eligible entities, which may require ninety (90) days of duplicate service, without billing for the new service.** Describe the specifics of how the Vendor plans to accomplish this requirement.

3.1.14.7 In addition to responding to the specific Hosted IP Voice solutions, often referred to as IP Centrex, as well the specific IP trunking requests in the pricing section, the vendor should list all VoIP, Hosted IP Voice, and IP trunks available as options in Appendix E. If the vendor provides any options other than the "Alternative access circuits" listed in Appendix C, they should provide pricing for these other options listed here in Appendix E. The vendor may advance their technical position by being able to offer a variety of IP trunking facilities; beyond the required T-1 to Ethernet 10Meg, such as DS-3. If provided, the supplemental pricing for these options shall remain firm throughout the life of the contract. If the Vendor's IP trunking is specific to a given IP enabled Voice CPE manufacturer, please state so, and to which systems they are designed to connect. The State desires, at a minimum, that the IP trunking listed in the pricing section be available to (compatible with) both Nortel and Cisco CPE equipment.

However, because County and other Municipalities are able, and encouraged, to utilize any contract resulting from the release of this RFP for new MPLS and associated services, accommodation of a variety of CPE manufacturers would be in the best interests of the Vendor, and the State as a whole.

3.1.14.8 The State of WV desires the following Hosted IP Voice Services as an optional case by case service for both complete Telephony "IP Centrex" and IP Trunking to be offered along with all other Access Circuits to the MPLS Network

The State of WV's target application includes Agencies and other qualified contract participants with the following:

- Advanced IP features and a desktop interface (web browser) for telecom managers to manage everyday functions such as moves, adds, changes, and deletes (MACD), as well as network applications
- Flexible growth choices, as afforded by the scalable and interchangeable products

- Require the cost savings associated with moving their voice traffic on to their (IP) networks
- The State does not want additional infrastructure investments or monthly maintenance costs

3.1.15 Hosted VoIP Service

3.1.15.1 **Features and Benefits Overview**

[Critical] The Vendor's Voice over IP (VoIP) portfolio of products shall provide customers the ease and efficiency of one network for both voice and data services. The Vendor's VoIP offering should provide a migration path to full Voice over Internet Protocol (VoIP) by offering VoIP Trunking/IP Integrated Access and pure IP Voice path Circuits with a full range of features like today's traditional PRI service. This is intended to allow customers to use their existing IP enabled private branch exchange (PBX) or key system. Additionally where the State WVOT deems applicable the Vendor will offer at fixed tiered pricing Hosted IP Centrex that has access to all of the voice and network features.

3.1.15.2 The Vendor's VoIP portfolio of products should, as applicable, include the following:

- A converged network for voice and data, reduced from two separate voice and data networks, which will lower costs.
- A converged voice and data should make network management easier. Any number of sites can be accessed from any location via the MPLS or Internet.
- Total cost of ownership should be reduced in comparison to traditional disparate networks; and administrative and end-user productivity gains can be realized through use of advanced IP features and functionality.

- The Hosted offering should have unlimited local and unlimited or tiered blocks of intrastate or interstate long distance minutes in 6 second increments or better. NOTE: All calls from existing DAIN to MPLS locations and vice versa are by definition intercom calls and therefore no charges should apply. This unlimited calling or tiered blocks should apply to all local, in-state, and interstate long distance to all fifty states. Tiered plans are acceptable between 1,000 minutes per month per voice path to unlimited minutes per month per voice path. However, in the cost analysis section, the vendor is required to quote the tiered plan block of minutes that fits the number of minutes required in the cost chart and in the case of tiered or blocked number of minutes, the vendor should quote the over plan cost per minute per voice path.

3.1.15.3 **[Critical]** Agency intra-MPLS (VoIP trunking or Host IP Voice service) to other non-MPLS Agency VoIP Trunking or Hosted IP Service calling should, by definition, be toll free. For intra-MPLS calling (i.e. for sites connected with VoIP, or the MPLS calling to sites not yet connected to the MPLS that are still on the DAIN, (existing Voice Network) these calls also **should** be toll free within WV.

3.1.15.4 The vendor, at a minimum, should offer the State WVOT two options for both VoIP trunking and Hosted IP Voice Service with respect to toll free service (Does not include 800 services).

3.1.15.4.1 **Option A:** Includes all types of VoIP trunks and Hosted IP Centrex Services offered that based on the number of possible voice paths or simultaneous calls from that Agency, on that VoIP circuit connected to the MPLS facility, that all 50 States will be unlimited toll free calling.

3.1.15.4.2 **Option B:** Allows Agencies with fewer LD minutes per month to receive a reduced rate on the VoIP trunks or Hosted Voice service, but cap the zero charge toll free to all 50 States in the US to 1200 minutes per simultaneous Voice path on said VoIP trunk or Hosted Voice Service. Describe in detail the Vendor's plans to accomplish the aforementioned. Vendors will be judged on both of these potential offerings in the pricing section on the three pricing scenarios, (Appendix B), however it is to the Vendor's advantage to offer even more options along these lines and provide pricing clearly referenced back to the section where the offering is listed in Appendix C and a list of corresponding pricing for said options only in Appendix D. These options will not affect the pricing section score, but may have a positive impact on the technical evaluation.

3.1.15.5 **[Critical]** The State of WV cannot accept double billing, therefore it is required that the MPLS Vendor provide the new MPLS VoIP trunking or Hosted IP Voice Service at no charge until the existing DAIN facilities are removed and billing has ceased. This is a "not to exceed" 30 days after installation of the new service. **Exceptions to this thirty (30) day limit are all E-Rate eligible services, which may require ninety (90) days.**

3.1.15.6 The Vendor's services and features should be managed through a familiar, web-based portal using intuitive click-and-point controls, including for easy moves, adds, and changes.

3.1.15.7 The Hosted Voice offering should include flexible growth choices and the ability to support remote locations since the service is scalable and interchangeable with other VoIP services.

3.1.15.8 The Vendor's Hosted IP Services offering should include "Call Blast" feature that allows users to be reached at a variety of locations and devices – anytime, anywhere, anyplace.
3.1.15.9 The Vendor's offering should include a variety of packages with and without CPE, and with and without Voice mail and Unified Messaging. The State desires these versatile service options, which provide the advantages of VoIP while eliminating the need for updating PBX equipment and the capital expenditure required for premise-based solutions.

3.1.15.10 **[Critical]** The following tables describe the strongly desired optional features the Vendor should provide with their IP Voice Service. These specifications represent industry standard features and functionality which may be contained in the Vendor's solution, but may potentially be described with different language, or slightly altered specifications. **Although these highly desired features are optional, it is REQUIRED that the Vendor address their availability or alternative, equivalent offerings, in this section. Failure to complete this section fully will result in point deductions in the final evaluation of this RFP.**

A detailed description of Call Types, Access Types, and Compression that should be supported by the Vendor's offering follows:

The Vendor should indicate if they provide the services, as described below, or if they offer a variance of these feature, including a description of how their offering varies from the provided description of the desired features and functionality.

Feature	Description	Vendor's Response
Outbound Long Distance Calls	Offers network gateways to the PSTN at the MPLS POP. The Vendor long distance telephone network, allowing the customer to complete off-net calls.	
Outbound Local Calls (network-based)	Customers can dial local calls from their Session Initiation Protocol (SIP) phone or public switched telephone network (PSTN) phone. Replaces the need for a connection to the Local Exchange Carrier (LEC). With the products ordered a la carte, users can have a Direct Inward Dialing (DID) number (public phone number) assigned to their SIP phone or a PBX phone behind an Enterprise gateway. Local number portability will also be supported.	
Outbound Local Calls (Customer Premises Solution)	Customers who are outside the Vendor VoIP local footprint can deploy a Cisco enterprise gateway on their premises, which enables them to dial local calls. With the products ordered a la carte user can have a direct inward dial (DID) number (public phone number) assigned to their phone behind an Enterprise gateway. Local number portability will also be supported.	

Inbound 8XX Calls	Basic toll-free routing and termination. Enhanced toll-free routing capabilities are not supported. Calls are rated at standard toll-free rates. Bills and reporting generated via standard toll-free systems.	
Dedicated Toll Free	With Dedicated Toll Free, the customer's Toll Free numbers terminate to the VoIP platform and are converted to Toll Free Nodes Based Routing.	
Fax	Support for fax pass-through.	
Remote calling into private dial plan	Ability to set up a remote call in number for private dialing plan	
Dial Plan Integration	Provides the flexibility to have VoIP and traditional sites share a common dial plan. Note: VoIP integration with is restricted to 7-digit dial plans only.	
Web Center	Web Center contact center services can be used in conjunction with VoIP.	

3.1.15.11 **Access Types**

Feature	Description	Vendor's Response
Internet Access	IA speeds available include T1 and T3 Internet Dedicated.	
Internet Access (IA) Shadow T1	Internet T1 Shadow is a redundant service option that provides an automatic back-up connection in the event of primary T1 failure.	
DSL Access	DSL speeds available include 384 Kbps and 768 Kbps. Note: Only SDSL is supported.	
MPLS	MPLS enables companies to share information across a MPLS backbone in a secure environment. MPLS service integrates the capabilities of layer 2 switching (ATM and frame relay) and layer 3 routing (IP) and evolves frame relay and ATM into IP-based services. MPLS access speeds available include 384K, 512K, 768K, T1, MLPPP/NxT1, and T3.	

3.1.15.12 **Compression**

Feature	Description	Vendor's Response
G. 711 Codec Support	Uncompressed voice (includes the bandwidth needed for frame or IP headers).	
G.729 and G.729A Codec Support	Compressed voice using the G.729 and G.729A codec (includes frame relay and/or IP headers).	

3.1.15.13 **Network Features for Subscribers**

Feature	Description	Vendor's Response
Anonymous Call Rejection	Enables a subscriber to reject calls from anonymous parties who have explicitly restricted their Caller ID. By activating the service via the Subscriber Web Interface, callers without available caller identification are informed that the subscriber is not accepting calls at that time. The subscriber's phone does not ring and the subscriber sees or hears no indication of the attempted call. This service does not apply to intra-location calls. Only deliberate anonymous numbers are rejected. Callers whose numbers are unavailable are not rejected. Callers that are rejected are informed that the called party is not accepting calls from unidentified callers. ("The party you are trying to reach is not accepting calls at this time.") Note: The caller will be blocked altogether. The caller will not be forwarded to voicemail for example even if the called party has the voicemail feature.	
Alternate Numbers	Enables an administrator to configure up to two additional phone numbers and/or extensions to a subscriber. Normal ringing is provided for incoming calls to the primary phone number and subscribers have the option of enabling a distinctive ring for calls to their second and third phone numbers. If distinctive ringing is enabled, distinctive call waiting tone will also apply. For outgoing calls from the subscriber, the subscriber's primary phone number is the calling line	

	identity.	
Automatic Callback	The Automatic Callback (ACB) service allows users to monitor a busy party and automatically establish a call when the busy party becomes idle. Upon reaching a valid ACB busy condition, the user will hear an announcement asking if they would like to monitor the line and be called back when it is idle. To activate ACB, the subscriber enters the digit prompted for then goes on hook. As soon as the called party becomes idle again, ACB attempts to re-establish the call between the subscriber and the previous busy party. The ACB service can only be activated against a destination within the same group.	
Blind Call Transfer	Enables a subscriber to transfer a call unattended before or after the call is answered. Subscribers can only execute blind call transfer from the Communication Manager. Note: When using the Cisco 1912, 7960, or 7940 phones, this call transfer feature can be negatively impacted if multiple incoming calls are received at the same time.	
Call Blast Personal	Call Blast enables subscribers to have multiple phones ring simultaneously when any calls are received on their VoIP phone number. The first phone to be answered is connected. Caller can also select to have simultaneous devices not ring while already on a call or ring on all incoming calls.	
Call Forwarding Always	Enables a subscriber to redirect all incoming calls to another phone number. If activated, a subscriber should specify the forwarding number. A status indicator on the Communication Manager identifies whether this service is enabled. Subscribers can also make their office phone emit a short ring burst to inform they are next to their phone when the call is forwarded by using the Ring Reminder.	
Call Forwarding Busy	Enables a subscriber to redirect calls to another destination when an incoming call encounters a busy condition. If activated, a subscriber should specify the	

	forwarding number.	
Call Forwarding – Multi-Phone	Multi-Phone call forwarding allows an end-user to specify a different forwarding number for each entry of Selective Call Forwarding.	
Call Forwarding No Answer	Enables a subscriber to redirect calls to another destination when an incoming call is not answered within a specified number of rings. If activated, a subscriber should specify the forwarding number and the number of rings before forwarding.	
Call Forwarding Selective	Enables a subscriber to define criteria that causes certain incoming calls to be redirected to another destination. If an incoming call meets subscriber specified criteria, the call is redirected to the subscriber specified destination. A criteria set is based on incoming calling line identity, time of day, and day of week. Multiple criteria sets can be defined. All criteria should be met for a call to be forwarded in this scenario. If all criteria are not met, the call is delivered as if service was not available. Up to 12 incoming numbers can be defined for forwarding.	
Call Notify	Enables a subscriber to define criteria that causes certain incoming calls to trigger an e-mail notification. If an incoming call meets subscriber specified criteria, an e-mail (or short message to a cell phone) is sent to the notify address informing the subscriber of the details of the incoming call attempt. A criteria set is based on incoming calling line identity, time of day and day of week. Multiple criteria sets can be defined.	
Call Park	Enables a subscriber to put a call on hold and then retrieve it from another station within the call pick-up group. To park a call, a subscriber depresses the flash hook and dials the call park feature code. The call is parked and the caller is held. To retrieve the call, the subscriber goes to any phone in the call pick-up group and dials the call retrieve feature code, followed by the subscriber's extension. The call is retrieved and connected to the retrieving subscriber. Subscribers can	

	also execute call park via the Communication Manager.	
Call Pickup	Enables a subscriber to answer any ringing line within their pick-up group. The administrator sets up the pick-up group which defines the set of subscribers to which the call pickup feature applies.	
Call Pickup Directed	Enables a subscriber to answer a call directed to another phone in their pick-up group by dialing the respective feature access code followed by the extension of the ringing phone.	
Call Pickup – Directed with Barge-in	Directed Call Pickup with Barge-in (DPUBI) allows users to dial a feature access code (FAC) followed by an extension to pickup (answer) a call directed to another user in the same customer group, or barge-in on the call if the call was already answered. When a barge-in occurs, a three-way call is established between the parties with the DPUBI user as the controller. Subscribers can configure themselves as barge-in exempt so their calls can not be barged in on.	
Call Return	To call back the last party that called, the subscriber dials the call return feature code. The system stores the number of the last party to call, and connects the subscriber to that party.	
Call Screening by Digit Pattern	Enables subscribers to specify digit patterns instead of individual phone numbers on the following selective services: Selective Call Forwarding, Selective Call Acceptance, Selective Call Rejection, Call Notification, and Priority Alert. Digit patterns consist of a sequence of digits followed by the * wildcard. For example, 240* would apply to any calls from phone numbers starting with 240. Also enables use of the "?" wildcard character in specifying digit patterns. The "?" wildcard character represents any single digit (0-9) and may be used multiple times anywhere within a digit string. The "?" wildcard may be used with or without the * wildcard at the end of the digit string. If the calling number is not available, the caller will get a network announcement	

	that says, "The party you are trying to reach is not accepting calls at this time."	
Call Transfer with 3-Way Consultation	To initiate Call Transfer with 3-way Consultation, the subscriber depresses the flash hook and dials the add-on party. When the call is answered, the subscriber depresses the flash hook and forms a three-way call with the add-on party and caller. To transfer, the subscriber hangs up causing the caller to be connected to the add-on party. Subscribers can also execute call transfer with three-way consultation via the Communication Manager. Note: When using the Cisco 1912, 7960, or 7940 phones, this call transfer feature can be negatively impacted if multiple incoming calls are received at the same time.	
Call-Waiting Enhancement	When a second call is received while a subscriber is engaged in a call, the subscriber is informed via a call waiting tone. If using IP Phones, there is also an indicator on the phone. To answer the waiting call, the subscriber depresses the flash hook. The subscriber connects with the waiting party and holds the original party. By depressing the flash hook, the subscriber reconnects to the original party and holds the waiting party. The feature completes when any party hangs up. Subscribers can also execute call waiting via the Communication Manager.	
Calling Line ID Blocking	The subscriber controls the service via the Subscriber Web Interface, which provides the ability to activate and deactivate the service. If activated, all calls made by the subscriber have the subscriber's identity blocked. Calling Line ID Delivery Blocking allows subscribers to block their number from being shown when calling other numbers except for intra-site calls which will always display the calling line ID. The feature can be enabled for all calls or it can be enabled selectively using the feature access codes.	
Calling Line ID Blocking per Call	In addition to being able to block the presentation of their Calling Line ID on all outgoing calls, subscribers also have the option of blocking on a per-call basis by dialing a feature code before making the call.	

Cancel Call Waiting/Call Waiting per Call	Allows subscribers with Call Waiting to deactivate/activate the operation of Call Waiting via the Subscriber Web Interface. In addition to being able to cancel call waiting for all incoming calls, subscribers also have the option of canceling their call waiting on a per-call basis by dialing a feature code before making the call, or after a switch-hook flash during the call.	
Communication Manager	The following features are included with the Communication Manager: Click-to-Dial Enables subscriber to input and dial a number, dial directly from a drop-down Phone List (Personal, location directory or Call Log) or Outlook tab, or click the Redial button. • Talk Enables subscriber, who is already engaged in call, to answer another waiting call. When available, Calling Line ID is displayed with caller's name (if available Dependent on names in the contact list and on-net status) and number. • Call Hold/Retrieve Enables subscriber to place an existing call on hold for an extended period of time, and then retrieve the call to resume conversation. While the calling party is held, the subscriber may choose to make a consultation call to another party. • Call Transfer Enables subscriber to redirect a ringing, active, or held call to another number or directly to voicemail. Before transferring the caller, the subscriber may choose to consult with the third party first or establish a three-way consultation. • Conference Enables subscriber to establish a three-way call involving two other parties. • Hang up Call Enables subscriber to disconnect a call that has been answered. • Configure Services Buttons are provided to enable subscriber to turn on/off frequently used services such as Call Forwarding Always and Do Not .	

	Disturb. Note: When using an IP phone as the terminating device, the Hold, Talk, Conference buttons are disabled (grayed out) on Communication Manager. Note: In order to use the Communication Manager, the user will have to download a java applet. Some companies configure their firewalls very strictly and prevent users from downloading java applications. In those cases subscribers will not be able to download the script and therefore will not be able to use the Communication Manager. Also note that if using Windows XP with SP2, the Vendor VoIP Application Servers may need to be added to the trusted security list in Internet Explorer.	
Communication Manager Express	Enables users to pre-configure multiple profiles for managing incoming calls differently based on the subscriber's status: • Available In the Office • Available Out of the Office • Busy • Unavailable Each profile includes preferences for managing the relevant incoming call functions (e.g., Call Forwarding (busy, no answer, always, selective), Simultaneous Ringing, Call Notify), which can be configured through a single easy-to-use web page or via the telephony user interface.	
Conferencing	Audio conferencing and Net Conferencing transported over The Vendor VoIP.	
Consultation Hold	To initiate consultation hold, the subscriber depresses the flash hook and dials the add-on party. When the call is answered, the subscriber can consult with the add-on party. To drop the add-on party and reconnect to the original party, the subscriber depresses the flash hook twice. Subscribers can also execute consultation hold from the Communication Manager.	
Distinctive Alert/Ringing	This is a feature of the Priority Alert and Alternate Number capabilities. When	

	setting the Priority Alert capability on, a distinctive ring will be given to those priority numbers. Likewise, when the Alternate Number feature is enabled, the user has the option of requesting a Distinctive Ringing when receiving a call from one of the Alternate Numbers. Distinctive ring is supported on the Cisco 7912, 7940, and 7960 IP phones. This feature is not supported for PSTN phones that utilize the Mediatrix Analog Gateway nor is it supported on the Uniden 200 IP phone.	
Do Not Disturb	Allows subscribers to set their station as unavailable so that incoming calls are given a busy treatment. Subscribers have the option to activate and deactivate the service by dialing a feature code or configuring the service via the Subscriber Web Interface. A status indicator on the Communication Manager identifies whether this service is enabled.	
Extension Dialing	Enables subscribers to dial extensions via their Communication Manager or phone to call other Subscribers at their location.	
Find Me – Personal	This is a feature that used to be supported and is now available again. This service sequentially attempts up to five phone numbers (in addition to, optionally, the base location) to reach the user. Upon triggering the Sequential Ring service, the callers are played an announcement stating to hold while the system is attempting to reach the user. The callers are then provided with ring back and comfort announcements, in sequence. The service sequentially tries the configured numbers until an answer is received, at which point the call is connected as usual. If all numbers are tried without receiving an answer, the caller is redirected to an overflow destination like voice mail. There is also an option to allow the caller to press a key to skip the search process.	
Flash Call Hold	Enables subscribers to hold a call for any length of time by flashing the switch-hook on their phone and dialing the respective	

	feature activation code. Parties are reconnected again when the switch-hook is flashed and the feature activation code is dialed again. To enable the feature subscribers flash the phone (press the flash button or press the hang up button once), dial the feature access code, and make the second call. The subscriber flashes the phone to toggle between the calls.	
Inbound Caller ID	Delivered information includes the caller's phone number. The information is delivered to the Subscriber Web Interface and the phone (if capable) only if the information is available and has not been blocked by the caller. Enables subscribers with Calling Line ID Blocking enabled to allow the delivery of their Calling Line ID on a specific call by entering the respective feature code (*65 default). Once the call is over, Calling Line ID Blocking is restored. Calling Party Name Delivery is available for On-Net calls to a SIP phone from another on-net SIP device.	
IP Phone Support	Subscribers can use SIP phones. Note: VoIP has certified select IP phones. Refer to The Vendor VoIP SIP Phones and Vendors for more information on the list of certified IP phones.	
Last Number Redial	Enables Subscribers to redial the last number they called by clicking the 'Redial' button on their Communication Manager or by dialing a feature code (e.g., *66).	
LDAP Directory Integration	The Lightweight Directory Access Protocol (LDAP) tab enables subscribers to click-to-dial a contact. It also allows subscribers to perform searches by contact name. This service may be integrated with an enterprise's own private directory. The LDAP database is queried by the Communication Manager to the customers Private LDAP Directory Server.	
Loudspeaker Paging	Enables subscribers to access an intercom paging system by dialing an extension at the location. The paging	

	system is configured as a subscriber and inter-connected via a standard two-wire interface.	
Multi-Path Forwarding	There are no limitations on the number of simultaneous calls a subscriber can forward. Calls are specified for forwarding via the web portal interface.	
Outbound Caller ID	Originating location sends Billing Telephone Number (BTN) of caller. Currently, station level Automatic Number Identification (ANI) is not available.	
Outlook Integration	This service enables subscribers to integrate their personal contacts in Microsoft Outlook with their Communication Manager. Using the Outlook Contacts tab in the Communication Manager, subscribers can perform a search of their personal Outlook contacts by name or company. Once the desired contact is located, subscribers may click-to-dial one of the contact's phone numbers or the subscriber may choose to display the contact's v-card by clicking their name. All the Outlook contact information is pulled directly from the subscriber's personal Outlook files. Essentially the Communication Manager, a java-based program, pulls all the appropriate information from the Subscriber's Microsoft Exchange server or personal computer (PC) each time they log onto Communication Manager. The Outlook contact info is automatically refreshed when the Communication Manager is accessed. Subscribers can also manually refresh it with a simple point and click on the Communication Manager screen. The Vendor suggests less than 1000 contacts in any single folder for optimal performance. VoIP supports Microsoft Outlook 2000 and 2002. The Communication Manager Outlook Integration is certified to work on Windows 98 Service Pack 2 and higher, Windows NT Service Pack 4 or higher, Windows 2000 Service Pack 1 or higher, and Windows XP.	
Personalized Name Recording	Name recording in conjunction with Auto Attendant. A .WAV file is recorded via	

	phone and then uploaded via the Vendor Customer Center Personal Dashboard web screen. Users can use any application to record the .wav file. The format should be a CCITT u-Law, 8.000 kHz, 8 bit Mono .wav file.	
Phone List Group	Each subscriber added to the location is automatically added to this group list. Also included are the extensions for reaching the Auto Attendant(s), and Hunt Group(s), when applicable. Using the Common Phone List Feature, the administrator can add additional phone numbers to the Group List by either adding them individually via their web portal or by importing them from a file. This flexibility would allow the administrator to create a directory that lists all Subscribers in the entire enterprise. The list can not be edited by Subscribers but it can be searched.	
Phone List Personal	Each subscriber can add, delete, edit and re-order numbers in their Personal Phone List, which serves as a personal speed dial list. Subscribers can add multiple numbers to this list by uploading them from a flat file.	
Phone List Call Log	The call log is accessed through the Communication Manager and includes the most recent numbers registered for each category, as well as the respective call times and dates.	
Printable Group Directory	The business group and contact information is displayed in one of two formats: Summary or Detailed. The Group Directory is accessible from the Vendor Customer Center Administrator Dashboard Portal or via each Subscribers Communication Manager.	
Priority Alert/Ringing	The subscriber sets the criteria (e.g., incoming calling number, time of day, and day of week) for determining which calls require priority notification via their The Vendor Customer Center Personal Dashboard web interface. Multiple criteria sets, or profiles, can be defined. The criteria for each Priority Alert entry can be a list of up to 12 phone numbers or digit patterns, a time of day range and specified days of the week. All criteria for an entry should be true for the phone to	

	ring with a different tone (phone number and day of week and time of day).	
Private Dial Plans	Many corporate customers depend on private dial plans to facilitate intra-enterprise communications. Company can assign their own private number plan between locations. VoIP can support private numbers up to 32 digits or can utilize an existing DAP-based dial plan.	
Remote Office	Enables subscribers to access and use their VoIP service from any end point, on-net or off-net (e.g., home office, mobile phone). Note: When using remote office, all feature codes should be entered using the Communication Manager rather than the home office or mobile phone.	
Ring Splash	Enables subscribers to have a short ring burst played on their phone when the following services are triggered: Call Forwarding Always, Call Forwarding Selective, and Do Not Disturb. Ring Splash can be enabled for each of these services individually and serves as a reminder that the respective service is active.	
Selective Call Acceptance	If an incoming call meets subscriber specified criteria, the call is allowed to complete to the subscriber. All other calls are blocked and the caller is informed that the subscriber does not wish to receive their call. The subscriber controls the service via the Subscriber Web Interface, which provides the ability to set the criteria sets for determining which calls are allowed to complete. A criteria set is based on incoming calling line identity, time of day, and day of week. Multiple criteria sets can be defined. Up to 12 phones numbers or digit patterns can be defined. All criteria should be met in order to be activated. If the calling party's ANI is not one of the numbers listed on the selective call acceptance list, the caller is played a standard recording, "The party you are trying to reach is not accepting calls at this time." Administrators can not modify the recording. Note: This feature is only available if the enterprise location is within the Vendor	

	local footprint.	
Selective Call Rejection	If an incoming call meets subscriber specified criteria, the call is rejected. All other calls are accepted. The subscriber controls the service via the Subscriber Web Interface, which provides the ability to set the criteria sets for determining which calls require blocking. A criteria set is based on incoming calling line identity, time of day, and day of week. Multiple criteria sets can be defined. Up to 12 phones numbers or digit patterns can be defined. All criteria should be met in order to be activated. If the calling party's ANI is one of the numbers listed on the selective call rejection list, the caller is played a standard recording, "The party you are trying to reach is not accepting calls at this time." Administrators can not modify the recording. Note: This feature is only available if the enterprise location is within the Vendor local footprint.	
Shared Call Appearance	All phones have the same extension on their phone and can view status of the line for all phones. Unlike alternate numbers which is a virtual termination, shared call appearance numbers should be physically provisioned on the subscribers phones. The first phone to be answered. If one of the phones is already hosting an active call under the Subscribers ID, incoming calls are delivered to the active phone and any outgoing calls from another phone using the same subscriber ID are blocked. Therefore if one of the users is on the Shared call Appearance extension the other users with the same extension will not be able to use the line. Example: Applications of this service include setting-up a second line for an executive assistant or in a secondary workspace (e.g., lab). Warning: Although lamp management is supported on the Polycom IP phones, Cisco and Uniden phones will not show the status of the call on their phone. They do not support lamp management. A common application for this feature is to have the same number on an executive	

	and administrator phone. Due to the lamp management limitation, an admin currently has no way of knowing whether the executive is on their phone by viewing a lamp on their phone.	
Speed Dial	If required, customers can request to have up to 100 frequently called numbers enabled for speed dial. Entry of the two-digit code is preceded by a configurable prefix: 0-9, A-D, *, or # (default). Subscribers can program the numbers in their directory via the Speed Dial page in their The Vendor Customer Center Personal Dashboard web portal, or directly through their phone using the respective feature access code (*75 default).	
Telephony User Interface	Enables subscribers to call from any phone and modify their call forwarding features, their Communication Manager Express features, or their Auto Attendant greeting. Administrators may also use the Telephony User Interface to record Auto Attendant greetings remotely.	
Telephony User Interface – Calling	This feature enhances the Communication Manager Telephony User Interface by allowing an authenticated user to originate calls. Once the Telephony User Interface authenticates the user, the user makes calls as if they were originated from their normal location. This means that services such as OCP, account/auth code and voice VPN will apply on the outgoing calls made from the Telephony User Interface. This also means that accounting records will be generated against the user's account. The user can make as many calls as desired. The user can either wait for the remote party to hang up, or hit an escape sequence to originate a new call from the Telephony User Interface.	
Three-Way Calling	To initiate a three-way call while engaged in a regular two-party call, the subscriber depresses the flash hook and dials the third party. Before or after the third party answers, the subscriber depresses the flash hook and forms a three-way call with the two parties. To drop the third party, the subscriber depresses the flash hook and is reconnected with the original party in a regular two party call. If the	

	subscriber hangs up, all parties are released. Subscribers also have the ability to execute three-way calls using the Communication Manager. Note: With Flash Call Transfer, the conference does not end when the phone is replaced on the hook, since the callers are transferred together.	
Voicemail	Network-based voicemail is provided. Voicemail accounts can be set up to provide company, per department and per subscriber accounts. Voicemail can be retrieved via phone, website or even e-mail.	

3.1.15.14 **Network Features for Administrators**

Feature	Description	Vendor's Response
Account Codes	Enables the tracking of calls made outside of the location by prompting subscribers for an account code. With this service, codes are not validated (see Authorization Codes). Administrators manage their account codes via their The Vendor Customer Center Location Dashboard web portal. There are three types of access: • Non-restricted Subscribers are exempted from providing an Account Code. • Restricted, Critical Usage Subscribers are automatically prompted for an Account Code whenever applicable. • Restricted, Optional Feature Access Code (FAC)-based Usage Subscribers are not prompted for an account code and instead (optionally) dial a FAC to specify an account code. If a subscriber does not enter a FAC, their call proceeds as usual. Voluntary Account Code Provides the option for subscribers to enter an account code for a call by dialing a feature code before the call, or by flashing the switch-hook during a call and then dialing the feature code (e.g.,	

	to register an incoming call from a client). Code Length is 214 digits.	
Administrator Web Dashboard	Web portal that empowers a business administrator to provision services for subscribers, a location, or the entire enterprise.	
Attendant Console	The web-based Attendant Console enables a subscriber (e.g., receptionist) to monitor a configurable set of subscribers. All should be built under the same location as the Attendant. The Attendant Console graphically displays subscribers status (busy, idle, do not disturb), as well as detailed call information. The Attendant Console window is integrated with the Communication Manager, thereby enabling the attendant to perform functions such as click-to-transfer or click-to-dial. • Filter Subscriber List Ability to filter the displayed list of monitored subscribers by name or title. • Jump to Name Enhanced ability to enter multiple letters of name to be displayed in console window via automatic scrolling. • Sort List In addition to sorting list by name, subscribers may also sort by title. • Configure Display Columns Flexibility to select which columns will appear on the monitored subscriber table, and in which order (e.g., name, title, number, extension, mobile, pager, status, e-mail). • View Call Information Option to view duration of monitored subscribers calls and name and number of parties that they are talking to. Note: There is no limit to the number of subscribers an attendant console can monitor at a location. The number of concurrent calls an attendant can handle at any given time however is dictated by the number of call appearances their phone can support and by their	

	geographic location.	
Authorization Codes	Prompts subscribers for an authorization code when making calls outside of the location. Calls will not be connected unless a valid code is entered. Administrators manage their authorization codes via their The Vendor Customer Center Enterprise Dashboard web portal. A subscriber can not have this service and the Account Codes service enabled at the same time. There are two types of access: • Non-restricted – Subscribers are exempted from providing an Authorization Code. • Restricted – Subscribers are automatically prompted for an Authorization Code whenever applicable. Code Length is 214 digits.	
Auto Attendant	The Auto Attendant serves as an automated receptionist that answers the phone and provides a personalized message to callers with options for connecting to the operator, dialing by name or extension, or connecting to up to six configurable extensions (e.g., 1 = Marketing, 2 = Sales, etc.). Configuration via the Vendor Customer Center Administrator Dashboard web interface also allows for hours of operation to be modified, with different options available for hours that the company is open or closed. Each VoIP location can have its own Auto Attendant and using the transfer function, Auto Attendants can be nested together creating a seamless nationwide Auto Attendant. (e.g., enterprises main Auto Attendant is configured to seamlessly route to the Auto Attendant of a particular department or location). If using the dial by name or extension option, the subscribers listed will be those associated with the specific location Auto Attendant. The auto attendant can now be configured to allow callers to dial an	

	extension from the first level menu. In addition, administrators can now allow name dialing from a combined first name and last name in addition to the last name and first name list.	
Auto Attendant – Enhanced Business Hours	The Auto Attendant can be set with multiple time ranges for example (9 a.m. - 11 a.m. and 1 p.m. - 2 p.m.) and support different hours on different days.	
Auto Attendant – Holiday Schedule	An administrator can create an unlimited number of Holiday schedules for their Auto Attendant. Up to a maximum of 20 dates or date ranges can be entered per schedule.	
Call Blast Hunt Group	Enables all of the phones in a hunt group to ring simultaneously when calls are received on a virtual number. The first phone to be answered is connected. This function is a routing capability of the Hunt Group feature.	
Calling Location ID Delivery	Provides the name and number of the location (or company) for outgoing calls from subscribers in the location, rather than providing the subscribers own name and number. The location number may be defined on a per subscriber basis.	
Calling Line ID Configuration	Enables the administrator to configure each of the displayed subscriber calling numbers. This information is visible to subscribers in their profiles as read-only.	
Calling Plan Incoming	The Incoming Calling Plan is configured via the Vendor Customer Center Location Dashboard web interface. In addition to being able to configure which types of calls each subscriber is restricted from receiving (e.g., intra-location), administrators may regulate incoming calling by restricting specific digit patterns. This is done with the Digit String feature in the administrator web portal. If a profile has not been configured for a particular subscriber, the default set of incoming call privileges for the location is applied. Use of the Custom Check Box on the administrator screen allows that subscriber to use their own call settings which can override location restrictions.	

	The Incoming Calling Plan also enables administrators to reject the following types of incoming calls: • Collect calls • Calls from within the location • Calls from outside the location Note: Calls can not be blocked by NPA-NXX.	
Calling Plan Outgoing	The Outgoing Calling Plan is configured via the Vendor Customer Center Administrator Dashboard web interface. In addition to being able to configure which types of calls each subscriber is restricted from making, administrators may regulate outgoing calling by restricting specific digit patterns. This is done with the Digit String feature in Administrator web portal. If a profile has not been configured for a particular subscriber, the default set of outgoing call privileges for the location is applied. Use of the Custom Check Box allows that subscriber to have separate call settings which can override the location level restrictions.	
Calling Plan Outgoing Enhanced	In addition to blocking or allowing given call types and digit strings, administrators have the following options for configuring the outgoing calling profile of their location and individual subscribers: • Authorization Codes Selected subscribers can be prompted for an authorization code to allow specified call types or digit strings. Administrators can pre-configure one or multiple authorization codes to be entered by subscribers. Use of this feature within the Enhanced Outgoing Calling Plan takes precedence over the standalone Authorization Code service. • Call Transfer Specified outgoing call types and digit strings can be automatically transferred to one of up to three transfer destinations that Administrators can pre-configure. For example,	

	international calls made from a conference room may be transferred to a company operator who will validate the Subscribers identity and their purpose for making an international call. Existing configurations are retained when the Enhanced Outgoing Calling plan is assigned to replace the basic version of the service. Provides Subscribers with the option to enter a Sustained Authorization Code to unlock calling from their phone. When the feature is enabled, subscribers will not be prompted for an authorization code every time they make a call that requires an authorization code, as defined by the Enhanced Operations Channel (EOCP). Separate feature access codes are used to turn this feature on and off. Note: Custom Subscriber may be selected in the Dashboard.	
Calling Plan Forwarded/Transferred	Enables administrators to prevent specified subscribers from forwarding or transferring calls to certain types of numbers, such as long distance, toll, or premium numbers. Calling plans are configured via the Vendor Customer Center Administrator Dashboard web interface. If a profile has not been configured for a particular subscriber, the default set of incoming call privileges for the location is applied.	
Configurable Extension Dialing	The extensions can be of any length (2 to 6 digits) as defined by the administrator and dialed via the Administrator Web Interface or by phone. All extensions within a location may be of the same length.	
Configurable Feature Codes	Provides each location administrator with the option to specify the feature codes (a.k.a., star codes) associated with their services (e.g., Last Number Redial, Call Return) via the Vendor Customer Center Administrator Dashboard web portal. Subscribers can see, but not edit, the star code associated with each service at any time by referencing their The Vendor Customer Center Personal Dashboard	

	web portal. Enables Administrators to configure two different feature access codes for the same service. For example, *69 and #81 could both be used to enable Call Return. Note: Feature access code can be two to five characters long; consist of digits (0-9) and the special characters * and #. The special characters can occur only in the first two positions; and the last character may be a digit.	
Configurable Feature Code Prefix	Enables the administrator to define up to two different prefixes to precede their feature codes. Each prefix may include 1-2 characters, with the default being a single star (*).	
Configurable Time Zones	A default time zone is specified for each location. The respective time zone is used for all services requiring date/time stamps, such as Auto Attendant and Selective Call Forwarding.	
Device Inventory	Enables administrators to inventory their equipment including premise gateways and IP phones via their The Vendor Customer Center Administrator Dashboard web interface. Devices may be easily added, deleted and modified. In addition, administrators can assign subscribers directly to a device and/or a port on a device.	
E911 Support Enhancement	Enables routing of emergency calls to the correct tandem switch based on the caller's phone number. The system ignores subscriber disconnects and disallows features to be used when an emergency number (i.e., 911) is dialed.	
Hunt Groups	Hunt Groups allow users to be included in a specified hunt group to handle incoming calls received by an assigned Hunt Group phone number. This is a virtual number not a specific subscriber telephone number. Administrators can choose from any of the following hunt schemes, each of which rings the specified phones in a different manner: • Circular sends calls in a fixed order. The call is sent to the	

	first available person on the list, beginning where the last call left off. The Circular option tries the agent after the last agent to take a call. The search continues including looping around the list until it reaches the agent it started with. • Regular sends calls to users in the order listed by an administrator. Incoming calls go to the first available person on the list, always starting with the first person on the list. • Call Blast all of the users in the group simultaneously; the first user to pick up the ringing phone is connected. • With Uniform, as a call is completed, the user moves to the bottom of the call queue in a shuffling fashion. The next incoming call goes to the user who has been idle for the longest. If a user receives a call that was not directed to them through the hunt group, the call will not be included in the receiving order for Uniform calls. • No Answer Timeout enables calls that have been distributed to a phone, but not answered in a specific number of rings, to be redirected to the next available phone. If all idle phones have been visited once without answer, there are two options for handling the call: forward call to an external number, or give the call a Temporarily Unavailable treatment, which can trigger a service such as voicemail. Note: There is no limit to the number of users that can be included in a hunt group. Note: Call forwarding features will not apply to calls within the hunt group. Likewise, incoming calls to the hunt group are never forwarded to the voicemail service assigned to a member of the hunt group. Remote Office features, however can be used in conjunction with a Hunt Group routing.	

THIS PAGE WAS INTENTIONALLY LEFT BLANK

Music on Hold	Enables administrators to upload an audio file onto the system to be played to parties on hold. Users can use any application to record the .wav file. The format should be a CCITT u-Law, 8.000 kHz, 8 bit Mono .WAV file. There is a 10 minute maximum threshold or approximately (4.7 meg).	
PS/ALI	Private Switch/Automatic Location Identification (PS/ALI) is an advanced form of E-911 service. It gives customers the ability to deliver station-level Automatic Number Identification (ANI) and exact location information to the Public Safety Answering Point (PSAP). For more details, refer to Emergency (911) Service with The Vendor VoIP.	
Series Completion	The Series Completion service can be assigned to a selected series of lines to forward calls on a busy condition. It is a form of hunting in which the next line in the series completion group is tried in a prearranged order, without any limit on the number of sequential forwards. Unlike hunt group functionality, the lead number for a series completion is associated with a specific subscriber. The call is only forwarded if the subscriber's line is busy. If the user's line is not busy then the network will route the call according to the rules that have been configured for a "no answer" condition. This service is used to support Key System functionality. Key systems typically ring all available lines in a specified order for incoming calls, regardless of the number dialed to reach the company. For example, when calling a tech support hotline, the subscriber dials (800) 555-HELP. That number attempts to ring line 1 of company. If line 1 is busy, it will attempt to ring line 2. If line 2 is busy, and so on. If all lines are busy, the call can be sent to or another assigned service of the series completion group. Similarly, if all lines or subscribers of this company were assigned to a Series Completion group, The Vendor VoIP acts just like a key system.	

3.1.15.15 **Management**

Feature	Description	Vendor's Response
Call reporting details via web screen	Billing reports can be generated daily, weekly, monthly for call detail and printable via website.	
Feature Reporting	Feature reports can be generated for Accounting and Authorization Code usage.	
Customer-managed Routers	The Vendor Business will design and implement service. Customer retains control of CPE management.	
• Administrative site management via web screen	Via the Vendor Customer Center, VoIP provides administrator accounts on a central website for setting up default feature classes for a range of users. Supported Browsers • Microsoft Internet Explorer 5.0 or higher with the Microsoft Java VM installed. The Vendor Business recommends 128 encryption for Secure Socket Layer (SSL) support on the browser. • Other versions of incoming exclusion (IE) or any version of Netscape Navigator may be compatible with the Communication Manager, but have not been tested. Recommended Screen Resolution 1024x768 resolution, 16-bit color depth.	
Multi-language Support	Screens can be displayed in multiple languages.	
• User self-provisioning and management via web screen	Via the Vendor Customer Center, VoIP provides web access for users to set up their phones and administer features and calling treatments. Supported Browsers • Microsoft Internet Explorer 5.0 or higher with the Microsoft Java VM installed. The Vendor Business recommends 128 encryption for SSL support on the browser.	

	• Other versions of IE or any version of Netscape Navigator may be compatible with the Communication Manager, but have not been tested. Recommended Screen Resolution 1024x768 resolution, 16-bit color depth.	

3.1.15.16 **Security**

Feature	Description	Vendor's Response
Authentication	Validates that user names and passwords to ensure only trusted users are on the network. For SIP phones and analog interfaces, authentication is performed by SIP digest user authentication. For a digital PBX with a router/gateway, authentication is performed via IP Security Authentication Header Protocol (IP Sec AH).	

3.1.15.17 **Signaling Support**

Feature	Description	Vendor's Response
SIP	Session Initiation Protocol, an open standard and the leading VoIP protocol.	

3.1.15.18 **SIP Phone Features**

Feature	Description	Vendor's Response
Do Not Disturb	SIP phones support Do Not Disturb.	
Hold	SIP phones allow users to place calls on hold.	
Consultation Hold	The user may place a call on hold and originate another call with privacy.	
Three-Way Conferencing	Ability to conference in a third party. Note: Compression will not be supported with this type of conferencing. Instead the call will be processed using the G.711 codec.	
Multi-line SIP Phones	SIP phones offer a minimum of two lines, with Cisco phones supporting up to six lines.	

DTMF Digit Support	Dual Tone Multi-Frequency refers to push button or touch-tone dialing.	
Phone Portability	IP phones may be plugged into any The Vendor VoIP location.	
XML Application Support	Can write specialized Extensible Markup Language (XML) applications to run on the Cisco phone.	
Call Log	Displays a log of placed, received, and missed calls.	
Last Number Dialed	Speed dials the last number dialed.	

3.1.15.19 **Disaster Recovery**

Feature	Description	Vendor's Response
Busy Out Monitoring	Cisco service within their Inter-network Operating System (IOS) that will continuously monitor a locally connected wide area network (WAN) interface in order to control a locally connected channel associated signaling (CAS) or Primary Rate Interface (PRI). If the WAN T1 alarms, then the router will place the CAS or PRI interfaces into a similar alarm state, allowing the PBX to route around to a more PSTN optimal path. Likewise when the WAN T1 comes up the router will place the CAS or PRI interfaces into an up state and calls will be completed over the VoIP network.	
Bypass Port	One default bypass port available to the PSTN in the event of a power outage or network outage condition. The Mediatrix bypass port will be activated if: • The unit is not able to register with the SIP proxy (including the case where the Registrar is not reachable or responding). • The local area network (LAN) link is not up; e.g., LAN cable disconnected for example. • Power failure. Following one of the above conditions, the unit will try to register every two minutes or as soon as the local area network (LAN) cable is reconnected.	

	When the units are able to re-register, the bypass will be deactivated after 10 seconds (if a call is not already in progress).	
Internet T1 Access – Shadow T1/Shadow T3	Internet T1/T3 Shadow is a redundant service option that provides an automatic back-up connection in the event of primary T1/T3 failure. A second T1/T3 is provisioned from customer premises to The Vendor IP backbone and Border Gateway Protocol (BGP) MEDs are used to reroute traffic in an outage situation. Customers may have their primary circuit with The Vendor Business. The T1/T3 Shadow circuit may be the same bandwidth as primary connection.	
Internet T1 Access – Diverse and Double	T1 Diverse is two T1s provisioned to different The Vendor-owned hubs. T1 Double is two T1s provisioned to the same The Vendor-owned hub and the same gateway router. Most customers route voice traffic to an IP/PSTN gateway which has one IP address. When a router has multiple outbound paths to the same destination IP address (as in T1 Diverse and Double) it selects only one of those paths for that destination. Once the router decides which T1 to use, all the traffic destined for the VoIP gateways will choose that same T1. The same situation exists for traffic in-bound to a customer. If substantially all of a customer's traffic is destined for one IP address, as when the customer has a firewall, the Vendor edge router will select one path and not use the other T1. Customer designs should take this into account. If the customer has predominately off-net traffic, which means that most of their traffic is going to single IP address, they will not receive a load-sharing benefit from T1 Diverse or Double. On-net traffic destined for various IP addresses, however, can router over either T1.	

77

3.1.15.20 **IP T1/PRI Trunking Generic [Critical]**

IP T1/PRI is designed for small-size Agencies & customers that simply need converged voice and data access and basic Class 5 calling features. This service works with existing IP Key/PBX systems, thereby eliminating the need to heavily invest in extra equipment. With IP T1, there is no need for equipment changeover or disruption to services. Customers will not need to retrain employees on any of the calling features or functions, and implementation is transparent to the end-user.

The Vendor may describe, in detail, their integrated Voice and Data T-1 on the MPLS, if this offering isn't available, describe what is available. (For instance the State requires IP trunking using G.729 codec.)

- The benefits of IP T1 should include:

- One converged network for voice and data, reduced from two separate voice and data networks, means lowers costs.
- A minimum of 40 simultaneous calls
- All the features of a conventional PRI, (like those used commonly from the DAIN contract)
- One network for voice and data also makes network management easier.
- Unlimited local and on-net calling with a bundle of off-net domestic long distance minutes within the 50 U.S. states offers cost savings.

3.1.15.21 **IP Trunking: Cisco Specific**

IP Trunking is designed for large customers with 200 or more employees, which have already invested in a Cisco CallManager 4.1.3 IP PBX. With IP Trunking, the customer's IP PBX is connected directly to the carrier's IP backbone, eliminating the need for the customer to purchase complex and costly Time Division Multiplexing (TDM) enterprise gateway customer premises equipment (CPE). IP Trunking provides converged access and the essential features that large customers require.

This offering's target market includes customers that:

- Have 200 to 1,000, or more employees
- Do not want to retrain employees on any of the calling features or functions; all the Cisco CallManager features are retained
- Do not want to invest in costly TDM gateway equipment infrastructure or desktop equipment
- Prefer to avoid equipment changeover or disruption to services
- Want the cost savings realized through converged access

3.1.15.22 **IP Trunking Ethernet, (over DS-3 or Alternate means)**

- Requires handoff to IP enabled PBX or Pure IP softswitch via Ethernet 10Meg
- Should accommodate up to 400 simultaneous calls
- Should have all traditional PRI DAIN type features.

3.1.15.23 **[Critical]** QoS and DiffServ Signaling: IP by itself is simply a best-effort service, not sufficient enough to provide the strict delay, jitter, and bandwidth guarantees required for voice over IP (VoIP) and other real-time traffic. WVOT requires that the proposed solution support a standards-based QoS or DiffServ aware TE mechanism when making forwarding decisions for passing VoIP traffic through tunnels. Confirm Vendor's compliance with this mandatory and describe the method for QoS or DiffServ TE signaling for VoIP traffic. (See real-time QoS in 3.1.7.3)

3.1.16 Statewide Remote User Access (Dial-up, DSL, et. al.)

3.1.16.1 Statewide Dial-up WVOT desires statewide dial-up access, DSL access, cable access, WiFi access, to support the development of a secure, highly functional and highly stable remote access solution for telecommuters, small remote offices and after-hours business workers.

3.1.16.2 Dial-up Access: WVOT desires that the Service Provider provide cost-effective access to the MPLS VPN network for remote users, field employees, travelers on temporary duty, temporary work sites, sites with outages, and home tele-workers without high speed connections. Such dial-up should be 56K or better and include v.90 and v.92 support. This dial-up capability could be provided via publicly available ISP service through the State's existing ISP WVNET, or through a private Vendor MPLS remote user network, whichever is most cost-effective. Describe Vendor's approach for providing cost-effective remote user access to the MPLS VPN network.

3.1.16.3 Remote Local Access: WVOT desires that remote users have the option of connecting to the MPLS VPN network either through a local dial number or via a toll-free access number. Describe Vendor's strategy to controlling costs by directing users to local numbers rather than more expensive 800 numbers. VPN via Internet DSL access for telecommuters – add language in this section.

3.1. 16.4 Capacity: The number of concurrent dial-up connections should be selectable, both by local dial numbers and toll-free access. Also, in time of an emergency, the need for remote access may dramatically increase. Describe Vendor's approach to appropriately sizing the capacity of dial-up network access to limit busy signals as well as providing additional local and toll-free numbers as necessary.

3.1.16.5 Availability: WVOT desires that remote user access to the MPLS VPN be readily available. Describe Vendor's approach to ensuring the Availability of remote user access.

3.1.16.6 Idle Time Disconnect: WVOT desires that the Vendor has an idle time disconnect feature. WVOT desires the ability to adjust the default period of time in which a statewide dial-up call is dropped due to inactivity. Describe how the Vendor will provide idle time disconnect capability. Describe how the Vendor's solution could allow WVOT to adjust the idle time disconnect interval.

3.1.17 Access Circuits

3.1.17.1 **[Critical]** Access Circuit Services: The local access connection between the customer premise equipment and the Service Provider's Point of Presence

(POP) should use generally and commercially available transport services. Preference should be given to open, secure, scalable, industry-standards-based, packeted services, such as Ethernet in 10 Meg/100 Meg and 1 Gig (both redundant and non-redundant), SONET, Frame Relay, ATM, Clear channel T-1 and DS-3 circuits and others, providing end-to-end QoS capable of transporting voice, video, and data applications within a converged media stream. TDM-based transport services, such as T1 digital carrier, ISDN, DSL, etc., shall be acceptable where dictated by the business needs (e.g. cost, SLA) of the agencies. (The State desires that the apparent successful Vendor leverage access facilities such as Ethernet over Frame Relay and ATM.) **Vendor should confirm their ability to meet this mandatory and fully describe their strategy for increasing desired access facility types.**

3.1.17.1.1 **[Critical]** User Perspective/Mesh Topology: The Provider should offer the option for meshed links, which will enable agencies to build redundancy in the WAN through a Mesh Topology. **Vendor should state any additional cost for adding VRFs or PVCs, and present these costs in the Cost Section of this RFP.**

3.1.17.2 **[Critical]** The State cannot pay for dual service therefore it is a requirement that the winning vendor install and test replacement Access circuits of any type at no charge until the legacy Data 05 or other service from any legacy Vendor is terminated. The services should meet all applicable industry standards pertaining to information security, and vendor should be willing to accommodate and comply with WVOT Enterprise Information Security Policy, as it evolves over time. The vendor is not obligated to provide the service at no charge after 30 days from Access Circuit installation. **Exceptions to this are K-12 and the Library Commission which are subject to E-Rate and will be converted last. They will require ninety (90) days without double-billing.**

3.1.17.3 Access Circuits: WVOT desires that the Service Provider supply the most economical physical Access Circuits that meet the service level and bandwidth requirements of the individual agencies. Describe the strategy for providing the most economical accessibility while meeting Service Level Agreements (SLA).

3.1.17.4 Availability: WVOT desires the ability to choose Access Circuit Availability per the business requirements of each service address. Use the pricing spreadsheet located in Appendix B which describes required access circuits, services, and/or service bundles. List any and all access types not on the required lists that are available and provide the pricing for said additional options in Attachment C, clearly labeled and referring back to this section. The State will require for all Access Circuit types the 5 previously mentioned CoS categories, except where a certain access type is "Best Effort only". (e.g. dial up, cable modem, DSL, and any Internet VPN access are "Best Effort" only if the four (4) FCC QoS Requirements are not applicable.) Specifics for each FCC category will be stated in the SLA with its accompanying bandwidth, Availability, Latency, Jitter, MTTR.

3.1.17.5 Bandwidth: The Vendor should specify the various types of access services offered, including the bandwidth increments and ranges. Does Vendor's offering enable the customer to specify their bandwidth requirement? If so, clearly define the various types of access services offered including the bandwidth increments and ranges.

3.1.17.6 Bandwidth on Demand: WVOT desires the ability to provide its customers with additional capacity on an Access Circuit, as necessary, to accommodate increases in traffic, such as a videoconference, or other special requirements. Describe the approach for providing this capability.

3.1.17.7 Ability to Add Wireless Access and Satellite Circuits: To fully support a mobile workforce and provide alternate connectivity where traditional land based circuits are not available, WVOT desires that the MPLS VPN network be able to add Wireless Access Circuits. This is not a request for the Vendor to build out a statewide wireless network but have the capability to connect wireless access circuits. List the types of wireless access circuits that the proposed solution (such as IEEE 802.11g, 802.16, Wi-Max, WiFi, VSAT, etc.) would support. Describe the security measures required to connect with the wireless access circuits.

3.1.17.8 **[Critical]** Third Party Circuits within the current and future network infrastructure: There are circuits that are provided by business associates and/or exempt agencies, to provide specialty services to WVOT and State agencies. Describe Vendor's approach for providing connectivity for these third party circuits, within the planned MPLS VPN. Describe in detail, the charges the Vendor is offering for third parties to connect to the MPLS peripheral Edge Router, Ethernet switch, or other Vendor-owned device for each access type, QoS, and port size, as listed in Appendix B. These include: ADSL to 1 GB switched Ethernet redundant real-time access circuits.

3.1.17.9 The Vendor should provide and hold firm this third-party port connection charges. These charges can, and should, be based on the same parameters the State's Access Circuits are charged, however, without the transport component. If a third party connects directly into the State of WV's core network or peripheral data center, the State will charge said third party, or State Agency, a similar fee to be retained by the State of WV. NOTE: The State acknowledges that the vendor cannot be responsible for third party vendors providing access to the MPLS.

3.1.18 Alternate Access

WVOT desires alternate access at some service addresses to provide for business continuity. These service addresses have application needs that dictate high levels of redundancy, fault tolerance, and disaster recovery. Describe Vendor's cost-effective approach to providing for high Availability at these sites.

3.1.19 Disaster Recovery

3.1.19.1 Loss of Data Center: In the event of a loss of the State's Data Center, Access Circuits should be provisioned in a manner that will allow WVOT or the Service Provider to swing circuits to an alternate Data Center. Describe Vendor's strategy for providing connectivity in such an emergency. This includes provision for the rapid establishment or upgrade of Access Circuits to one or more alternate data centers, rapid establishment of temporary PVCs to the alternate site and rapid label propagation in support of the new PVCs. **Please define vendor's interpretation of rapid establishment.**

81

3.1.19.2 Agency Service Address: In the event of the loss of an agency service address of WVOT or one of its customers, the Service Provider should be able to reestablish connectivity to existing site and rapidly provision access connectivity to an alternate site. Re-provisioning an existing site may include either site mappings alone, or may include site mappings, physical transport, and CPE. Describe Vendor's strategy for providing connectivity to an alternate site in case of such an emergency. Include timelines, provisions for the rapid establishment or upgrade of Access Circuits to the alternate site, rapid establishment of temporary PVCs, and rapid label propagation in support of the new PVCs for all classes of service.

3.1.20 **Internet Access (Response is Optional)**

3.1.20.1 The State of West Virginia's current ISP provides Internet access on 4 OC-3s in the North, and 4 OC-3s in the South, which feed up to 1.2GB worth of user endpoints via these two POPs, via the current Network described on page 26. The State of West Virginia desires that the Vendor proposes potentially multiple alternative(s) and ideally superior designs in terms of naturally redundant Internet connectivity and Internet speed and performance for the dollar spent here in this section. Please remember to provide pricing for any and ALL "Optional Internet/ISP connectivity" in the Optional pricing Appendix E. Describe here what makes the Vendor/Carrier a Tier 1 ISP Provider? Does the carrier have, at a minimum, an OC-48 backbone reaching both US coasts Metropolitan Area Ethernet POPS? Has the carrier's backbone been in existence for at least six months? Does the carrier own at least 80% of the fiber facilities on its Internet backbone? If not, why is the Vendor described as a Tier 1 ISP Provider?

3.1.20.2 Alternate Internet Access: In order to provide protection against failures and emergencies, and to ensure business continuity, WVOT desires options for a second, alternate connection, to the Internet via a separate Internet Service Provider. Identify the provider and describe the approach. The MPLS carrier is encouraged to do this at the PE router in Charleston thus eliminating the requirement for the second OC-3 to the Internet carrier at the Capitol complex vault. The MPLS Vendor is encouraged to provide any and all alternate Internet configurations that will result in no degradation of Internet service or security yet will reduce long-term costs and subsequently will reduce the amount billed back to each Agency for Internet service. Please provide as much detail as possible and provide how the vendor would transition to any proposed alternatives. The Vendor needs to keep in mind that K-12 and the State Library Commission have filters in place at WVNET and the Vault and these Agencies will need to maintain control over said Filtering and other aspects of their VRF(s) or individual VPN(s).

3.1.20.3 It is highly desirable that the State of West Virginia contract include options for connectivity of the MPLS network to the evolving Internet2 backbone as it evolves from Abilene to the replacement on 2007-2008. It is understood that organizations and agencies within the State may need to secure membership in Internet 2, to take advantage of such a connection.

3.1.20.4 It is Highly Desirable that the State of West Virginia contract includes options for connectivity of the MPLS network backbone to multiple Tier 1 National Commodity ISPs, and includes options for service redundancy, diverse paths, load balancing and bandwidth optimization. Please describe, in detail, how the Vendor's solution would address this desirable.

3.1.20.5 It is Highly Desirable that the State of West Virginia contract with a Vendor who facilitates peering arrangements with multiple in-state broadband ISPs. This desirable is in an effort to promote West Virginia ISP services, and facilitate efficient and optimal utilization of commodity Internet bandwidth into, and out of, the state.

3.1.21 **Universal Services Fund – Network Configuration**

3.1.21.1 Support for Universal Services Fund: The Universal Services Fund (USF) provides communities across the country with affordable telecommunication services. The Universal Services Administrative Company (USAC) manages the fund. The Schools and Libraries Universal Service Support Mechanism (E-Rate) provides discounts to assist most schools and libraries in the United States in obtaining affordable telecommunications and Internet access. Rural Health Care is a universal service support mechanism that provides reduced rates to rural Health Care Providers (HCPs) for telecommunications services related to the use of telemedicine & tele-health.

3.1.21.2 **[Critical]** USAC Compliance: The Service Provider should provide an MPLS network that will allow the Schools and Libraries in West Virginia to qualify for Universal Services Administrative Company (USAC) Funds. The network should also allow the Rural Health Care Providers in West Virginia to qualify for Universal Services Administrative Company (USAC).

- Describe how the proposed solution complies with the Universal Services Fund requirements for E-rate and Rural Health Care.
- Provide Vendor's Service Provider Identification Number (SPIN).
- Provide evidence that the Vendor is an Eligible Telecommunications Services Provider, as defined by the State of West Virginia.
- Confirm that Vendor offers E-Rate eligible entities discount billing in accordance with FCC guidelines.

3.1.21.3 **[Critical]** Universal Services Fund – Filings: The Service Provider should comply with current and future Universal Service Fund submission requirements. (See http://www.universalservice.org).

3.1.22 **Network Security**

3.1.22.1 The physical security of network components (such as buildings, power services, continuity of operations, etc.) and the security of the information that will traverse the network are of prime concern and should be defined as part of this proposal. Redundant infrastructure components within the core network will be valued highly and should be highlighted within the proposals. Agreement to comply with WVOT and other State policies concerning Information Security and Physical Security, both existing and future, will be a requirement for an award, and continuation of any contract throughout its designated term.

3.1.22.2 Compliance with WVOT Enterprise Information Security Policies: The Service Provider should comply with all WVOT Enterprise Information Security Policy with respect to the network, personnel, information, facilities and applications as they relate to this RFP. Describe the security infrastructure provided with the proposed MPLS, and demonstrate how it addresses WVOT's Enterprise Information Security needs. www.wvgot.org.

3.1.22.3 Support WVOT Information Security: Describe how Vendor will work with the WVOT to address security threats. This includes threat mitigation and event correlation and access to tools and reports to aid WVOT in monitoring and tracing security threats. This also includes providing support for forensic investigation.

3.1.22.4 Intrusion Controls: The vendor should provide all requested support/cooperation to the WVOT in the implementation of any intrusion control technologies. Vendor should state their compliance with this desirable.

3.2 MPLS VPN Management and Monitoring

3.2.1 **Evolving and Emerging Technologies:** WVOT desires that the Service Provider have a method for incorporating evolving and emerging technologies. A Technology Plan is one method of achieving this goal. Describe how evolving and emerging technologies are addressed and the approach taken to incorporate changes into the overall MPLS VPN architecture.

3.2.2 **Ongoing Technology Refresh**

3.2.2.1 A paramount concern of the MPLS VPN initiative is to obtain a Service Provider committed to providing services under a philosophy of rapidly accommodating change. This is commonly referred to as "future proofing." Further, WVOT is seeking long-term professional assistance that is committed to meeting newly defined service needs and technological advances within advantageous timeframes and within a framework of cost effectiveness. WVOT envisions migration of existing Data 05 circuits onto the MPLS VPN architecture to be completed by the end of June 2008. It is desired that VoIP be made available as a service offering approximately three months after the initial MPLS VPN architecture is established and continue migration from the existing Centrex/DAIN onto the MPLS IP Voice throughout the life of the MPLS contract and renewals. Please respond with vendor's ability to meet these timelines.

3.2.2.2 Technology Refresh: Describe how technology refresh will be addressed in support of the MPLS VPN for data, VoIP, multimedia services and CPE managed by the Service Provider (Hosted IP Voice and Video services or monitoring, encryption, filtering traffic management and any additional optional services): Vendors should take care to make sure and address the pricing of any and all quoted options in Appendix E unless requested specifically in the pricing sheets (Appendix B). The vendor should include hardware upgrades or replacement, modifications to CPE IOS as a service wherein the CPE is owned and maintained by the MPLS vendor except where the Agency has procured their own Voice Data and or Video CPE. In such cases the Agency or the WVOT will be responsible for maintaining said CPE from the Vendor from which it was procured. In some cases this may be the same Vendor that supplies the MPLS, but will be in no way tied to the MPLS requirements or SLA unless the CPE is provided as a turnkey service: i.e. Hosted Voice solutions. The MPLS vendor may be requested at quoted billable rates in the optional pricing section to provide modifications to routers and switches that support the MPLS VPN. Identify those components that will be updated and reconfigured prior to the initial deployment of MPLS VPN service in order to accommodate technology refresh.

3.2.2.3 Security Technology Refresh: WVOT desires that the Service Provider

manage and operate within manufacturers' security requirements across the entire MPLS VPN for the life of the contract. Describe management of the MPLS VPN from a security refresh standpoint.

3.2.3 **Operational Planning**

Operational Planning: The Service Provider should facilitate a forum that includes WVOT when planning for routine maintenance outages, CPE upgrades, changes to MPLS VPN Access Circuits, required technology refreshes and intrusive troubleshooting and testing. Describe procedures used for each and how WVOT will be incorporated into the planning process. Address the planning process for proactive and preventive maintenance programs.

3.2.4 **Maintenance Requirements**

3.2.4.1 **[Critical]** The successful vendor shall be responsible for the on-going maintenance of the MPLS Core and its Peripheral Edge Routers, Regional or Central Office based Ethernet Switches and all other Peripheral Edge devices as well as all circuits and services such as Hosted Voice Services, even those that may utilize a third-party to provide the "last mile". The successful Vendor will also be responsible for maintaining adequate bandwidth on the MPLS core and Peripheral Edges as well as the ability to increase circuit size and CoS in all regions to ensure adequate potential for rapid expansion as described in the SLA.

3.2.4.2 **[Critical]** Scheduled maintenance should occur on an advance mutually agreed upon time table that has minimal to nominal impact to the existing agency or entity . The vendor should state their maintenance window (e.g. 2a.m. to 5:30a.m.)

3.2.4.3 **[Critical]** Vendor should provide at least ten (10) calendar days advance notification, in writing (e-mail), to The Office of Technology's Help Desk and the Telecom Customer Service and Billing, (TCS&B), designee and or exempt Agency designee as assigned by the WVOT's TCS&B team's designee, of any scheduled maintenance affecting the State's private MPLS. The WVOT will then disseminate this information internally.

3.2.4.4 **[Critical]** In the event of required emergency maintenance, affecting the MPLS Network, the vendor shall inform both the Help desk and appropriate WVOT TCS&B designee OR, a WVOT-authorized Agency designee, and receive verbal approval prior to working on the circuits or any infrastructure that may affect the traffic flowing across the MPLS and any and all circuits VPN(s), VRF(s) etc. State the vendor's compliance with the above requirements, addressing each individually.

3.2.5 **Maintenance for Service Provider-Managed CPE**

3.2.5.1 Maintenance for Service Provider-Managed CPE: Describe maintenance policies and procedures regarding CPE that will be used in the delivery of MPLS VPN service to WVOT. Describe the preventive maintenance routines, equipment swap-outs, the remove-repair-return procedures, and how activities are coordinated in advance with the agencies. Identify available service levels and terms of coverage. This service

provider managed CPE is optional and in many cases the Agency or the WVOT will perform these tasks, however as stated earlier in cases where the service involves CPE, such as hosted Video services or Hosted IP Centrex the Vendor will be responsible for said CPE and should state compliance with this requirement.

3.2.5.2 **[Critical]** Note: Particular items in Appendix B require pricing for both Provider-Managed and Agency-Managed CPE options. It is critical to your Pricing section score to complete ALL of Appendix B with straightforward and specific answers. Appendix D is expected to be concise as well and directly reference the technical section of the RFP where the optional service, with or without CPE, was initially addressed.

3.2.6 **Maintenance for Agency-Managed CPE**

Maintenance for Agency-Managed CPE: This will be the responsibility of the Agency or the WVOT unless specifically arranged in a separate contract with a third party or the winning MPLS service provider.

3.2.7 **Configuration Management**

3.2.7.1 Configuration Management: Describe any system or application proposed for Configuration Management of Service Provider-Managed CPE configurations. Describe how the systems and applications operate. Describe procedures and methodology associated with configuration management.

3.2.7.2 **[Critical]** Configuration Records: Pursuant to the requirements of West Virginia State Code §5A-6-1, §5A-6-2, §5A-6-4, §5A-6-5, §5A-6-6, §5A-6-8, §5A-6-4a, §5A-6-4b, §5A-6-4-c and §5A-7-4 (Senate Bill 653), WVOT requires that current and accurate configuration records be kept for MPLS VPN access circuits and optionally managed CPE by the Service Provider at all locations. Describe Vendor's approach to maintaining these records and providing access to these records to WVOT.

3.2.7.3 Archiving Configuration Information: WVOT desires that all CPE configurations be archived on a regular basis. Describe the process and frequency proposed. Describe the policies affecting the retention periods and the depth of versions kept to include restoration testing. Clearly distinguish between transport and CPE configurations.

3.2.7.4 Security Configuration Management: Describe methodology and procedures to ensure the MPLS VPN is kept current with security patches or upgrades.

3.2.7.5 Rapid Modifications to Configurations: Describe the process and methodology for rapid modifications of configurations (rapid being within 5 days of notification). Address the time intervals required for change to occur for each type of configuration affected. (e.g., hosted voice Centrex, WAN Access Service Connection)

3.2.8 **Dynamic and Manual Rerouting Tracking**

[Critical] Dynamic and Manual Rerouting Tracking: WVOT requires that the vendor provide dynamic and manual rerouting tracking. Describe how dynamic

and manual rerouting will be monitored, detected in the MPLS VPN, and how WVOT will be notified.

3.2.9 **Monitoring**

3.2.9.1 **[Critical]** Monitoring: WVOT requires around-the-clock monitoring of services for the MPLS VPN Core, Peripheral Edge, and all circuit types utilized to reach customer/Agency premises **except** those deemed "Best Effort Only" in QoS (e.g., all Internet VPNs, ADSL and SDSL to the MPLS). This includes operating a Network Operations Center (NOC), utilizing state-of-the-art monitoring tools, performing real-time analysis and diagnostics of accumulated traffic information and extending to WVOT real-

time access to these tools so that WVOT is able to manage data, voice and multimedia MPLS VPN services. Vendor should clearly state and describe your approach or means of compliance.

3.2.9.2 **[Critical]** Service Providers' NOC: The Service Provider should provide and operate a network operations center (NOC) that performs network monitoring for the MPLS VPN twenty-four hours a day, seven days per week. Describe the NOC that will be used and the type of activity WVOT can expect from this NOC. Further identify which NOC will serve WVOT and the MPLS VPN. Describe how WVOT technical staff will communicate with Service Provider technical staff in the NOC, including telephone, e-mail, and other online contact. Identify which secondary NOC, if any, will be used as a backup.

3.2.9.3 **[Critical]** Alarm and Alert Monitoring System or Application: WVOT requires that an alarm and alert system that receives, processes and displays alarms and alerts received from Access Circuits and hardware, be used in the delivery of the MPLS VPN. Confirm Vendor's compliance with this mandatory and describe in detail, the system that will be utilized and how it will support WVOT.

- The vendor shall proactively inform the State of any serious issues.
- Clearly identify the capabilities of the system for generating alarms and alerts.
- Provide examples of output from such system or application screen-shots.
- Describe policies and procedures that are followed to notify WVOT once major or catastrophic alarms/alerts are received.
- Describe the backup system if one exists.

3.2.9.3.1 Viewing Alarms and Alerts: Describe what types of alarms and alerts are available for viewing and how and when they are generated.

3.2.9.3.2 It is highly desirable that the WVOT have access to a web-based GUI or other online interface for alarms and alerts.

3.2.9.3.3 Time Intervals: Identify time intervals Vendor has established that determine when an outage has occurred.

3.2.9.3.4 Reaction to Alarms: Describe what immediate steps are taken once an alarm is received.

3.2.9.3.5 Recurring Events: Describe what procedures are in place to mitigate recurring events.

3.2.9.3.6 Scope of Monitoring: Clearly identify, with examples, at what point in the transport architecture monitoring ends.

3.2.9.4 The State strongly desires that the Alarm/Alert system integrate into the Trouble Ticketing System: Is the alarm and alert system or application integrated into the Trouble Ticketing System used to support the MPLS VPN so that Trouble Tickets can automatically be opened when an alarm or alert is discovered? Describe the relationship between the two systems or applications and identify what constitutes a Trouble Ticket being opened once the information is forwarded from the alarm and alert system or application.

3.2.9.5 **[Critical]** Performance and Error Monitoring of MPLS VPN Access Circuits and Vendor Provided MPLS CPE except where noted (e.g., any "Best Efforts" circuits or services, ADSL and SDSL). WVOT requires that the Service Provider operate a real-time, modern performance and error monitoring system that will be used in the delivery of the MPLS VPN. Describe in detail, the system provided and how it will be used to support WVOT and the MPLS VPN. Provide examples of output from such system or application screen-shots. Describe policies and procedures that are followed to notify WVOT once major or catastrophic performance issues are encountered. Do not use monthly averages. The WVOT requires that these statistics be real-time, or as close as possible. Please describe vendor capabilities.

3.2.9.5.1 Degradation of service: Identify specific types of performance information that is being evaluated and how degradation of service is determined.

3.2.9.5.2 Reaction to Performance Issues: Identify the immediate steps that are taken once there is degradation of service or errors encountered and the procedures that are in place to address these events.

3.2.9.5.3 Time Intervals: Define how long a problem should exist before it is reported.

3.2.9.5.4 Problem Continuum: Identify what types of performance issues and errors are reported immediately and those that are monitored for a period of time.

3.2.9.5.5 Scope of Monitoring: Identify, with examples, at what point in the transport architecture monitoring ends.

3.2.9.6 **[Critical]** Bandwidth Utilization and Exception Monitoring: WVOT requires that the Service Provider operates a real-time, modern bandwidth utilization and exception monitoring system that monitors bandwidth utilization and creates exception reports to be used in the management of the MPLS VPN. Agencies should have real-time view only access to their locations and their VPNs/VRFs.

- ❖ Please describe the system in detail and how it will be used.
- ❖ Describe how WVOT will be notified when exceptions have been encountered that impact service delivery.

3.2.9.6.1 Traffic Usage by Technology-Type: Address specific performance monitoring criteria as it pertains to data, VoIP, and video bandwidth usage. Address each performance aspect individually, showing what is measured and how it is measured

3.2.9.6.2 Polling Intervals: Identify polling intervals used for each technology-type.

3.2.9.6.3 Threshold Levels: Provide threshold levels observed for each technology-type including the latency time window adopted that generates an exception.

3.2.9.6.4 Time Interval: Define how long a problem should exist before it is reported.

3.2.9.6.5 Problem Continuum: Identify the types of exceptions that are reported immediately and those that are monitored for a period of time.

3.2.9.7 Redundant Performance and Error Monitoring System or Application: Describe and address the relationship between the primary and secondary system or application, if a redundant system or application is proposed.

3.2.9.8 Application-Layer Monitoring: For diagnostic purposes WVOT desires the ability to occasionally view or monitor application-layer traffic traversing the MPLS VPN. WVOT desires to monitor end-to-end response times as applications are released over MPLS VPN in order to determine application performance levels. Describe time intervals that can be included in a report. Indicate whether or not the report can be accessed and displayed via web browser.

3.2.9.9 Verification of MPLS VPN Traffic Processing: WVOT desires that the Service Provider operates a real-time, modern system that captures and displays data, VoIP, and video traffic that is deployed across the proposed MPLS VPN architecture in accordance with applicable Service Levels. Describe how the system or application operates to display the MPLS VPN usage.

3.2.9.10 **[Critical]** Access to Alarm and Alert System or Application: It is required that Internet-connected WVOT users be able to access the alarm and alert system or application with a web browser. Identify any other needed hardware or software for access to the alarm and alert system or application. The alarm and alert system or application should provide a graphical user interface to the web browser. Agencies should have real-time read only access to their locations. This system or application should support at least twenty (20) concurrent authorized WVOT users.

3.2.9.11 Identification Options within Alarm and Alert System: WVOT desires to have the flexibility to view alarm and alert information by identifiers recognizable by WVOT. Examples are Agency Name; Circuit ID, VPN, and CPE name. Describe how the system offers this flexibility.

3.2.9.12 **[Critical]** Alarm and Alert System or Application Training: Training should be provided as to access and use of the alarm or alert system or application. Training should be provided for at least 50 (fifty) WVOT users. Describe the training.

3.2.9.13 Alternate Access to Alarm and Alert System or Application: WVOT desires a practical alternative means of access to the alarm and alert system or application. Describe how this is accomplished.

3.2.9.14 Access to Performance and Error Monitoring of MPLS VPN Access Circuits and CPE: WVOT strongly desires that their users be able to access and view performance of the error monitoring system or application with a web browser. WVOT prefers that the users only have access to their Agency information not the entire MPLS VPN network. Identify any other needed hardware or software for access to performance and error monitoring system or application. The performance and error monitoring system or application should provide a graphical interface to the web browser. This system or application should support at least 50 (fifty) concurrent authorized WVOT users.

3.2.9.15 Identification Options within Performance and Error Monitoring System: WVOT desires the flexibility to view performance and error monitoring information by identifiers recognizable by WVOT. Examples are Agency Name; Circuit ID, VPN, and CPE name. Describe how the system offers this flexibility.

3.2.9.16 Monitoring Data Filtered: Is information that is contained in alarm and alert data or performance and error monitoring filtered before it will be disseminated to WVOT? If yes, describe what is being filtered before it reaches WVOT.

3.2.9.17 Extracting Information from CPE Owned and Managed by Service Provider, (i.e. as a service like Hosted Voice solutions): WVOT desires direct secure access to CPE hardware used in the delivery of MPLS VPN service. WVOT would poll CPE and re-process that information on WVOT's own network management system. Describe WVOT's level of access, types of output, the frequency of polling allowed and the method allowed to poll data (SNMP, SNMPv2, SAA, etc.).

3.3 Trouble Ticketing

3.3.1 **[Critical]** WVOT requires that the Service Provider operate a Trouble Ticketing Function that includes an online system available statewide. The Trouble Ticketing Function should include processes and procedures that can be used by WVOT to open, update, close and track Trouble Tickets for the planned MPLS VPN and related services covered in this RFP.

3.3.2 **[Critical]** Trouble Ticketing System: WVOT requires that all trouble ticket activity initiated by WVOT that affects the support of MPLS VPN service delivery to WVOT should be done through an online Trouble Ticketing System provided by the Service Provider. The system should be available for use by WVOT twenty-four hours per day, seven days per week excluding maintenance time. Confirm Vendor's compliance with this mandatory and provide applicable policies and procedures used to support this system.

3.3.3 Trouble Ticket Activity Types: Identify the types of items and activities that flow through the Trouble Ticketing System and how open ticket confirmations are communicated back to WVOT.

3.3.4 **[Critical]** Notification Back to WVOT: Describe how WVOT is kept current on the progress of trouble tickets that were opened by the Service Provider and by WVOT.

3.3.5 Affect on SLAs: Define the time relationship between opening of a trouble ticket and the effects on supported SLAs, i.e., when do the SLA requirements begin?

3.3.6 Severity Levels: Describe how Trouble Tickets are treated differently based upon their Severity and Priority Levels. (Severity refers to the technical impact of a problem. Priority refers to the degree of business necessity for resolving the problem.)

3.3.7 Chronic Problems: Provide policies and procedures of how a problem becomes defined as chronic, and the resolution. Clearly identify time intervals between chronic events before a trouble ticket is opened.

3.3.8 **[Critical]** Advanced Outage Notification: WVOT should be notified prior to a planned outage affecting WVOT's MPLS VPN network, Access Circuits, CPE, or other associated IP-based services including video conference services. WVOT requires at least ninety-six (96) hours prior notice for short-term, routine outages. Provide a policy that complies with this requirement. List maintenance window types, time frames allotted, and identity which windows are excluded from any calculations of Availability.

3.3.9 Emergency Maintenance Windows: Provide the procedure as to when and how Vendor will notify WVOT when emergency maintenance is required.

3.3.10 Trouble Ticketing System Integration: Describe how the Trouble Ticketing System is integrated with Vendor's Order Management, Change Order, Provisioning, Performance Monitoring, Problem Management, and Billing Systems.

3.3.11 Access to Trouble Ticketing System: It is strongly desired that Internet-connected WVOT users be able to access the Trouble Ticketing System with a web browser. Identify any other needed hardware or software for access to the Trouble Ticketing System. The Trouble Ticketing System should provide a graphical interface to the web browser. Agencies should have real-time read only access to their locations. The Trouble Ticketing System should support at least twenty (20) concurrent authorized WVOT users.

3.3.12 Alternate Access to Trouble Ticketing Function: WVOT desires a practical alternative means of access to the Trouble Ticket System. Describe how this is accomplished.

3.3.13 Trouble Ticketing System Training: Training should be provided for access and use of the Trouble Ticketing System. Training should be provided for at least 50 (fifty) WVOT users. Describe the training that will be offered.

91

3.3.14 Redundant System or Application: Describe how WVOT would access the Trouble Ticketing System if the primary was unavailable. Address the relationship between the primary and secondary systems.

3.3.15 Identification Options within Trouble Ticketing System: WVOT desires the flexibility to track Trouble Tickets by identifiers recognizable by WVOT. Examples are Agency Name; Circuit ID, VPN, service address, CPE name. WVOT desires that the Service Provider be able to recognize and flag open Trouble Tickets by individual Circuit ID or customer for quick identification and prioritization by the proposed system. Describe how the Trouble Ticketing System addresses the above items.

3.3.16 Trouble Ticketing Tracking: Describe how WVOT would track Trouble Ticket status with as close to real-time reporting as possible. Clearly identify what can be tracked, by what identifier, and how that information is communicated back to WVOT.

3.3.17 Problem Resolution Process: Provide policies and procedures that address the process of problem resolution from time of initial incident to closure. Identify published response times for each level of resolution. Define WVOT's involvement.

3.3.18 Service Restoration: Describe procedures with respect to service restoration both for MPLS VPN Access Circuits and hardware, including CPE provided by the Vendor as part of the service. Address levels of Severity and Priority if applicable.

3.3.19 Troubleshooting and Testing: Describe the troubleshooting and testing procedures in place to support the integrity of the MPLS VPN, including MPLS VPN access and managed CPE operating in a production environment. When is troubleshooting initiated? Include what time of day troubleshooting is conducted for non-emergencies. Provide data parameters that indicate when tolerance levels for bandwidth utilization, errors, drops, round trip response time, and Jitter reach levels that require troubleshooting.

3.3.20 **[Critical]** Intrusive Testing: WVOT requires that the Service Provider notify WVOT prior to any intrusive troubleshooting or testing on Access Circuits and CPE used to support the MPLS VPN when a trouble ticket does not exist for same or if the circumstance does not require immediate intervention. Provide policy and guidelines for intrusive testing.

3.3.21 **[Critical]** Trouble Ticketing System Reports: The Trouble Ticketing System should be able to produce both scheduled and ad hoc reports and provide web browser access for WVOT. Provide screenshots of standard reports. Describe creation of ad hoc reports with the Trouble Ticketing System.

3.3.22 Alternative Access to Trouble Ticketing Reports: Describe how to access reports if WVOT is not able to retrieve reports online.

3.3.23 Trouble Ticketing Reporting: Is the information disseminated to WVOT filtered for content before it reaches WVOT? If yes, describe what is being filtered before it reaches WVOT.

3.3.24 Customized Reports: WVOT desires to create customized reports either on-demand or a scheduled basis. Describe the capabilities of the Trouble Ticketing System

in this area. Below are examples of reports that WVOT would be interested in generating (reports to include, but not limited to):

- Number of troubles reported within time frames: Time of day, day of week, month of year.
- Number of repeat troubles reported within a thirty-day period.
- Trouble Tickets by Agency
- Mean-time-to-repair statistics for all Priority Levels.
- By type of trouble reported as defined by Service Providers' classifications.
- By Priority Levels.
- Troubles reported by site ID, circuit ID, originator's name or ID.
- Number of troubles that were escalated by level of escalation.
- Number of trouble tickets opened by Priority Levels.
- Number of trouble tickets closed by Priority Levels.
- Number of trouble tickets unresolved by Priority Levels.
- Access into trouble ticketing system by user.
- Bandwidth utilization (in, out, and total)
- Latency
- Jitter
- Packet Delivery

3.4 **Reporting**

3.4.1 **[Critical]** Reporting: WVOT requires web -browser access to online reporting as it pertains to performance of MPLS VPN services. Examples of needed reports include alarms and alerts, threshold exceptions, user access, trend analysis, chronic Access Circuits or CPE, threat analysis, verification of traffic processing, etc. Describe the reports available and differentiate between reports that are scheduled and those that are available on demand. Provide example screenshots of the various reports and describe WVOT's options with respect to viewing (GUI, text, diagrams, etc).

3.4.2 **[Critical]** Report on Verification of MPLS VPN Traffic Processing: The Service Provider should provide WVOT with verification that MPLS VPN traffic is being processed at QoS and CoS levels prescribed by WVOT. Reporting should be broken down by agency and VRF/VPN at a minimum. Provide screenshots of this report.

3.4.3 Event Correlation on MPLS VPN Transport: Describe how event correlation analysis is conducted and how the results of the efforts are applied. Provide procedures that describe when event correlation analysis is initiated and how the results are applied.

3.4.4 Proactive Monitoring on MPLS VPN transport: Describe how the result of the event correlation analysis of the MPLS VPN transport is utilized to prevent future service affecting events.

3.4.5 Proactive Monitoring on CPE Managed by the Service Provider: Describe how the result of the event correlation analysis of the Service Provider managed CPE transport is utilized to prevent future service affecting events.

3.4.6 Proactive Analysis: Describe how the Trouble Ticketing System is used in support of the MPLS VPN. Describe if both transport and CPE Trouble Tickets are used in analysis.

3.4.7 Root Cause Analysis on MPLS VPN Transport: Describe how root cause analysis is conducted for the MPLS VPN transport and how the results of the efforts are applied. Provide policies that determine when root cause analysis is initiated and how the results are applied.

3.4.8 Root Cause Analysis on CPE Managed by Service Provider: Describe how root cause analysis is conducted for the Service Provider managed CPE and how the results of the efforts are applied. Provide policies that determine when root cause analysis is initiated and how the results are applied.

3.4.9 Trouble Ticketing System Integration: Describe how the Trouble Ticketing System is used to support the efforts to arrive at root cause analysis.

3.4.10 Trend Analysis: Describe how trend analysis is conducted on MPLS VPN Access Circuits and managed CPE. Provide policies and procedures that drive when trend analysis is initiated and how the results are applied.

3.4.11 Degradation of Service: Describe how degradation tracking of MPLS VPN Access Circuits is accomplished and examples of the types of Access Circuits tracked. Provide thresholds that trigger opening of a trouble ticket and provide remediation. Describe any variations of tracking as it pertains to data, VoIP and video.

3.4.12 Escalation: List and describe trouble Severity and Priority Levels and how they apply to data, VoIP and video applications. (Severity refers to the technical impact of a problem. Priority refers to the degree of business necessity for resolving the problem.) Provide examples for each. Describe Vendor's escalation polices and procedures for data, VoIP and video (if different) troubles and what drives troubles to be escalated to the next level. Identify professional skill levels that are required to perform each level of escalation. Describe communication methods that will be used by WVOT to track initial escalations and escalations between Severity and Priority Levels.

3.5 Service Ordering

Service Orders

3.5.1 **[Critical]**: All requests for service under this contract shall be submitted to the successful vendor by WVOT, or a WVOT authorized entity, via a TCR, as described in the CURRENT ENVIRONMENT section of this RFP. No service shall be installed by the successful vendor without a TCR that has been approved by WVOT. The vendor's failure to conform to this requirement may result in non-payment of services. The Vendor shall communicate electronically, at a minimum, once per week to WVOT with the TCR number, the vendor's work order number, and the due date of installation for all TCRs received from WVOT and or an authorized agent. TCRs will not be submitted by the State for the conversion of existing service. They will only be submitted when requesting new circuits, new features on existing circuits, etc.

3.5.2 The successful vendor should have a Network Operations Center (NOC) or equal with a 24 x 7 x 365 availability with on-duty network engineers that can be reached via a nationwide toll-free phone number. All calls into the NOC should be answered by a live operator (i.e. no IVR or Automated Attendant). As part of the RFP response, the vendor should also provide other appropriate contact information where problems or outages are to be reported. Upon such a report, the vendor shall note the time of the report, assign a reference number for the report, and provide this information to the caller.

3.5.3 The State requires the NOC (or equal) to have access to a current data base that includes all of the State's circuits, VPN(s), VRF(s), and all connected VoIP services whether Hosted or an IP trunk and or other future addition to said contract and by the same as mentioned above for the MPLS' complete range of attachments/access(s) and services by their physical location, name of the site, Circuit ID(CID), VPN, and or VRF ID etc., for easy identification purposes. The database shall be searchable by CID or other unique identification number or physical address.

3.5.4 **[Critical]** Escalation and reporting procedures for service outages shall be provided by the successful vendor(s) prior to award. Escalation schedules shall contain escalation timeframes from point of incident and telephone numbers for all levels of activity on the escalation schedule. Trouble call management escalation may include high priority reporting and resolution centers and not necessarily individuals. **The State requests that all this information be included with the vendor's response to the bid. The Vendor is to State that they can comply with the State of WV's required Service Order implementation and management requirements and is encouraged to provide any additional OPTIONAL means of automating and increasing effectiveness of the process.**

3.5.5 **[Critical]** The vendor should provide a statistical report of network reliability, excess bandwidth capacity at the MPLS Core and Peripheral Edge that, at a minimum, is to be presented at the WVOT/Vendor scheduled meetings. The State may require from time to time reports by geographic region showing capacity to turn up additional circuits and or services. The Vendor should establish thresholds based on the number and size of the Geographic area served that alert the WVOT and or its authorized Agency designee of when said threshold has been reached or breached. The State may request such statistical reports outside of the meeting times. If so, such reports shall be given to the State within three (3) business days from the date requested. **Describe in detail how the vendor plans to meet or exceed the aforementioned.**

3.5.6 Examples of reports are excess bandwidth capacity, network access type availability and reliability (all types), outage durations (all types), and measure of provisioning commitment. Summary reports will be prepared in graphical format and, statistical backup, on a per incident report, and per geographic region as applicable, will be made available. **Describe in detail how the vendor plans to meet or exceed the aforementioned.**

3.5.7 Service Order System Training: Train-the-trainer training should be provided to the WVOT staff as to access and use of the Service Order System. Training should be provided for at least 10 (ten) WVOT users. Describe the training that will be offered.

3.5.8 Service Order System Reports: The Service Order System should be able to produce both scheduled and ad hoc reports and provide online (web browser) viewing by WVOT. Describe the standard reports available. WVOT should be able to develop and view customized reports using the Service Order System. Examples of Service Order reports may include but not limited to Service Order activity by site, agency, specific time periods, order status, or by type of activity or circuit. Describe how the Service Order System can satisfy this requirement.

3.5.9 Provisioning of Additional MPLS VPN Service: Describe processes and procedures for engineering (preparation) of MPLS VPN services, Access Circuits, and other related services described in this RFP for the delivery of MPLS VPN service. Describe initial engineering, installation, configuration, testing, cutover, acceptance testing and billing establishment. Identify when the billing cycle begins. Detail coordination of activities with WVOT, including, but not limited to, site preparation (site survey) and establishment of access arrangements with other providers.

3.5.10 WVOT Requests for Engineering on Agency-owned CPE: Some WVOT Customers will purchase their own CPE. It is desirable that the Service Provider accept WVOT requests for new service that would require the Service Provider to configure agency-owned CPE for data, VoIP, and video for initial MPLS service delivery. Describe capabilities for engineering and configuration services for support of agency-owned CPE.

3.5.11 **[Critical]** Inventory: Service Provider should maintain a current and accurate inventory that would incorporate all the contents provided in Appendix C. Examples of items to be included, but not limited to: Circuit ID, IP, IP assignments for VPNs, CPE IOS, QoS/COS assignments, Service Address, Agency, on-site contact information and Access Circuits. The Service Provider should provide inventory information to WVOT on a regular basis and on request. The Service Provider should maintain a current copy of inventory to include service items once the deployment of MPLS VPN services begin. Inventory information should be available for secure viewing via web browser as well as in spreadsheet format on portable storage media (CD). Provide the policies and procedures around this requirement.

3.6 Service Provider's Help Desk and Network Operations Center

3.6.1 WVOT will operate the first level of support through the WVOT Help Desk but will require the vendor's Help Desk support as required. WVOT will act as the liaison and will "own" the problem on behalf of WVOT Customers. Some Agencies/customers will be authorized by the WVOT to interact with the vendor on their own behalf for their VPNs/VRFs and, potentially, billing. Vendor should state their willingness to provide the desired helpdesk functionality to all WVOT authorized users.

Describe the scope of help-desk coverage offered to WVOT personnel. Include the type of assistance that would be extended to WVOT for end-to-end network support, including connectivity and performance, for data, VoIP, and video technologies. Describe personnel qualifications and expertise that are offered in support of the technologies mentioned above, to include the various levels of Help Desk support for WVOT such as Tier 1, Tier 2, Tier 3, and describe the services offered for each level of service.

3.6.2 Help Desk Integration: The Service Provider should have specific Help Desk staff support that functions logically within the overall WVOT enterprise helpdesk scheme to support network services including video conference services. A single call into the support service structure should cover questions concerning performance, reservations and scheduling, as well as typical end-to-end problem resolution for multimedia services. Requests for assistance could occur at any time day or night. Describe the approach for supporting this requirement.

3.6.3 The successful vendor should have a Network Operations Center (NOC) or equal with a 24 x 7 x 365 availability with on-duty network engineers that can be reached via a nationwide toll-free phone number. All calls into the NOC should be answered by a live operator (i.e. no IVR or Automated Attendant). Describe the process used to contact live support at the NOC. As part of the RFP response, the vendor should also provide other appropriate contact information where problems or outages are to be reported. Upon such a report, the vendor shall note the time of the report, assign a reference number for the report, and provide this information to the caller.

3.6.4 **[Critical]** The State requires the NOC (or equal) to have access to a current data base that includes all of the State's circuits, VPN(s), VRF(s), and all connected VoIP services whether Hosted or an IP trunk and or other future addition to said contract and by the same as mentioned above for the MPLS' complete range of attachments/access(s) and services by their physical location, name of the site, Circuit ID, VPN, and or VRF ID etc. for easy identification purposes. The database shall be searchable by CID or other unique identification number or physical address.

3.7 Moves, Adds, Changes and Deletions (MACD)

3.7.1 **[Critical]** MACD Charges: WVOT requires that all charges associated with any work order activity will appear on the invoice to WVOT within a maximum of two (2) billing cycles from acceptance date. WVOT will not accept any MACDs that were not authorized by WVOT, or a WVOT-authorized designee. Describe Vendor's process.

3.7.2 **[Critical]** Travel Costs: Travel costs / per diem for Service Provider for services under this agreement will not be paid by WVOT.

3.7.3 The vendor should describe in detail the MACD capabilities that can be performed by the WVOT to reduce vendor work order charges.

3.7.4 The vendor should describe the access the WVOT will have to the MACD data base to determine the status of requested changes.

3.8 Change Orders

3.8.1 Change Order Function MACD (Moves, Adds, Changes, and Deletions): WVOT desires that the Service Provider operate a Change Order Function, which includes an online system (web browser). The Change Order Function should include processes and procedures that can be used by WVOT to request and track changes to

the planned MPLS VPN and related services covered in this RFP. Describe the function and how it will be used.

3.8.2 Change Order System: WVOT desires that all MPLS VPN Change Orders be entered through an online system (web browser) provided by the Service Provider. Describe how Change Order system fulfills this requirement. Describe how Change Orders are treated differently based upon their Priority Levels Examples of Change Orders would include, but not be limited to, MPLS VPN Core, Access Circuits, and CPE configuration changes, QoS/CoS prioritizations, Bandwidth increases. Clearly identify all turn-around times tied to each type of change order. Provide applicable policies and procedures used to support this system including alternate access methods if web is unavailable. Identify the types of items and activities that flow through Vendor's system and how confirmations are communicated back to WVOT.

3.8.3 Change Order System Integration: Describe how the Vendor's Change Order System is integrated with Order Management, Provisioning, Problem Management, and Billing Systems.

3.8.4 Access to Change Order System: WVOT desires that Internet-connected WVOT users be able to access the Change Order System with a web browser. Identify any other needed hardware or software for access to the Change Order System. Describe access to the Change Order System. The Change Order System should provide a graphical interface to the web browser. The Change Order System should support at least 40 (forty) concurrent authorized WVOT users.

3.8.5 Change Order System Training: Training should be provided as to access and use of the Change Order System. Training should be provided for at least forty (40) WVOT users. Describe the training that will be offered.

3.8.6 Change Order System Reports: The Change Order System should be able to produce both scheduled and ad hoc reports and provide online (web browser) viewing by WVOT. Describe any standard reports available. WVOT should be able to develop and view customized reports using the Change Order System. Examples of Change Order reports may include but not limited to Change Order activity by site, agency, specific time periods, order status or by type of activity or circuit. Describe how this can be achieved utilizing the Change Order System.

3.8.7 Hardware Changes to CPE Managed by Service Provider: Briefly describe the process for normal and emergency changes to hardware installed on an agency's premise (CPE.) Provide policies and procedures as to how the Change Order Function addresses hardware swap-outs, card and cable replacement. Describe policies for hardware repairs, replacements, swap-outs and update of inventory records. Provide lead times for service based upon different types of requests.

3.8.8 Configuration Changes to CPE Managed by Service Provider: Describe the process whereby normal and emergency changes are initiated by the Service Provider that affect configurations installed on an agency's premise. Include policies and procedures as to how the change management process addresses, but not limited to, routing tables, VPNs, ACL's, etc.

3.8.9 Restoration of CPE Configurations Managed by Service Provider: Describe Vendor's ability to accommodate a WVOT request to restore configurations to a Service Provider managed CPE device in order to bring a device back to its previous operational settings in the event of failure.

3.9 MINIMUM CONTRACT MANAGEMENT & BILLING REQUIREMENTS

Account Management Teams (Local and NOC) Numbers

The successful vendor is desired to provide appropriate LOCAL personnel, but at a minimum regional personnel to provide overall account management and to work in tandem with the dedicated MPLS NOC team and dedicated staff at WVOT and or Agency personnel granted authority to act on behalf of only their particular Agency or Agency(s) in the case where said Agency has been granted authorization by the WVOT. The Account Manager(s) will meet with WVOT staff on a regular basis to discuss contractual matters, technology planning, billing issues and other administrative matters. The timing and location of these meetings shall be determined by WVOT after the contract is awarded. If a phone conference is agreeable, it will be the vendor's responsibility to provide a conference bridge at no cost to the State.

This account management function shall include a single point of contact (SPOC) for all problem resolutions, billing issues, installation activity and maintenance. The single point of contact shall be available to state staff via nationwide toll free calling. Escalation procedures for account management personnel should be provided in response to this RFP and will be required from the successful vendor(s) prior to award. This shall include, but not be limited to, the escalation as a result of an outage, installation and/or billing matters. Escalation schedules should contain names, titles and telephone numbers of account management escalation personnel.

Describe in detail how your company proposes to meet or exceed our minimum requirements stated above for the Account Management Teams and their interaction with Authorized WVOT or Agency personnel. Describe in detail how your Account Teams are going to guarantee they are talking to an actual WVOT Authorized entity/person, (for instance, the WVOT Network Engineering team). Describe any proposed safeguards that would prevent an errant directive from any one authorized person or entity from either catastrophically affecting their VRF(s)/VPN(s), CoS, IP Voice Services etc or any other Agency's VRF(s)/VPN(s), CoS, IP Voice Services etc.

3.10 **Billing**

3.10.1 **[Critical]** WVOT requires that Vendor provide WVOT a point of contact for all billing issues/inquiries including a toll free number and email address. Collection agencies or collection departments are not allowed to contact WVOT. All communications will go through the Service Provider's single point of contact. The noted exception to this would be WVOT-authorized personnel, pre-approved to receive direct billing, who will require a like, single point of contact. Describe the process for this meeting this requirement.

3.10.2 **[Critical]** All billings for services installed under this contract shall be presented to the TCS&B team of the (WVOT) of the Department of Administration, unless the WVOT has authorized and directed the Vendor to allow Administration and billing to be direct from and correspondingly billed to a given Agency. The billing should

be both electronically and in paper format, on a monthly basis and accurately billed in accordance with the contract terms and pricing.

3.10.3 **[Critical]** Electronic billing shall be provided to WVOT in a format that is acceptable to the WVOT. The State reserves the right to request a sample of the Vendor's proposed electronic and paper billing prior to award from the apparent winning Vendor and the apparent second best total value Vendor. The Vendor should have technical support available to WVOT for the purpose of identifying the record layout, etc. so that invoices/reports can be generated from such electronic data.

3.10.4 The Vendor is required to provide a web based portal for the WVOT to view all contract participants inventories, bills and VPN9s), and VRF(s), including such detail as the Agency or Entities circuit Access types and CoS etc. Certain Agency's will be given permission by the WVOT to access only their specific Agency's portion of the VPN(s), VRF(s), circuits Access types, CoS etc, and their corresponding billing for their services. The granting of said access is at the sole discretion of the WVOT.

3.10.5 **[Critical]** The vendor shall be required to comply with the terms of West Virginia State Code, §5A-7-4a, (Senate Bill 700) and the emergency Legislative Rules with regard to billing and payment. For a copy of the Senate Bill visit: http://www.legis.state.wv.us/legishp.html. To view the emergency rules (you should have Adobe to view the rules), visit: http://www.wvsos.org/adlaw/proposed/161-02%20er.pdf

3.10.6 **[Critical]** Pursuant to the terms of West Virginia State Code, §5A-7-4a, (Senate Bill 700), spending units that do not pay through the State's Treasury are not required to be included in the billing submitted to WVOT. The vendors should offer the contract prices to non-state entities that are West Virginia County or City Municipalities, and or qualified non-profit entities, and bill their spending units directly for the services. (WVOT should be consulted prior to the vendor providing this direct billing, for authorization.)

3.10.7 Describe in detail how the vendor plans to meet, or exceed, the aforementioned requirements.

3.11 Billing Cycle

[Critical] All billings for services installed under this contract shall be presented to the TCS&B team of the (WVOT) of the Department of Administration, unless the WVOT has authorized and directed the Vendor to allow Administration and billing to be direct from and correspondingly billed to a given Agency. The billing should be both electronically and in paper format, on a monthly basis and accurately billed in accordance with the contract terms and pricing.

Electronic billing shall be provided to WVOT in a format that is acceptable to the WVOT. The State reserves the right to request a sample of the Vendor's proposed electronic and paper billing prior to award from the apparent winning Vendor and the apparent second best total value Vendor. The Vendor should have technical support available to WVOT for the purpose of identifying the record layout, etc. so that invoices/reports can be generated from such electronic data.

The Vendor is required to provide a web based portal for the WVOT to view all contract participants' inventories, bills and VPN(s), and VRF(s), including such detail as the Agency or Entities circuit Access types and CoS etc. Certain Agencies will be given permission by the WVOT to access only their specific Agency's portion of the VPN(s), VRF9s), circuits Access types, CoS etc, and their corresponding billing for their services. The granting of said access is at the sole discretion of the WVOT

The vendor shall be required to comply with the terms of West Virginia State Code, §5A-7-4a, (Senate Bill 700) and the emergency Legislative Rules with regards to billing and payment. For a copy of the Senate Bill visit: http://www.legis.state.wv.us/legishp.html To view the emergency rules (you should have Adobe to view the rules), visit: http://www.wvsos.org/adlaw/proposed/161-02%20er.pdf

As per the terms of West Virginia State Code, §5A-7-4a, (Senate Bill 700), spending units that do not pay through the State's treasury are not required to be included in the billing submitted to WVOT. The vendors should offer the contract prices to non-state entities that are WV County or City Municipalities and or qualified non-profits and bill their spending units directly for the services.
Describe in detail how the vendor plans to meet or exceed the aforementioned

3.11.1 Bill Cycle: Describe the bill date cutoff process.

3.11.2 **[Critical]** New Service Billing: WVOT's obligation to pay shall begin only after WVOT accepts the service ACCEPTANCE: The performance period shall begin on the installation date and shall end when the installed services have met the standard of performance for a period of thirty (30) consecutive days. The standard of performance shall be as proposed in the vendor's SLA. In the event the installed services do not meet the standard of performance during the initial thirty (30 consecutive days, the standard of performance test shall continue on a day-by-day basis until the standard of performance is met for a total of thirty (30) consecutive days. If the installed services does not meet the standard of performance after one hundred and twenty (120) calendar days, from the installation date, or the first day from the start of the performance period if such is delayed by the State, the State may at its option request to terminate the order and seek alternative plans.

3.12 **Invoice Presentation**

3.12.1 Categorization: Propose a billing hierarchy that presents invoice details categorized by the following:

-Rollup to statewide (WVOT)-

- WVOT regions
- Agency (total)
- Agency by site
- Agency Division
- Site (service address and CLLI code)
- Circuit type
- Circuit ID

101

3.12.2 **[Critical]** Circuit ID: WVOT requires all invoice components (e.g. FCC charges, one time charges, credits, recurring charges, cancellations, escalations, etc.) be linked to a Circuit ID.

3.12.3 Changes to Categorization: Describe process for changing the billing hierarchy after the initial set up.

3.12.4 **[Critical]** Sample of Categorization: Provide a sample invoice of no more than ten (10) pages demonstrating understanding of the requirements previously listed. The WVOT desires submission of both a hard copy and an electronic copy.

3.12.5 Electronic File Format: The vendor should provide to WVOT an requires the electronic submission of a single monthly invoice covering the entire State account in the format proposed in 3.10.3 that is able to be downloaded to an office application (such as: XML, RTF, HTML, XLS) and be searchable by every data field and service code. The vendor should have a web-based portal where the billing information is available without having to download the electronic invoice. Vendor should confirm compliance with this requirement and describe the proposed methodology.

3.12.6 Audit Support: WVOT desires that the Service Provider provide an accurate, reliable and secure monthly bill (both hard copy and the electronic version) and a process for monthly auditing of the bill. Confirm Vendor's compliance with this desirable and describe the proposed methodology.

3.12.7 Itemization: WVOT desires that invoices be presented in an itemized format with all abbreviations described. Service Provider should supply a current glossary (and describe process for maintaining the glossary) of all abbreviations for any and all invoice components.

3.12.8 **[Critical]** Penalties: WVOT will not be held liable for penalties of any kind, including, but not limited to; interest on late payments, cancellation charges and early termination charges. Confirm Vendor's acknowledgement and agreement. The State will adhere to the requirements of the Prompt Payment Act which governs interest on late payments.

3.12.9 **[Critical]** Records: WVOT requires that the service provider will, and will require each of its subcontractors, to maintain accurate books, records, documents and other evidence concerning its financial status, costs, expenses, formulas for computing prices, and provision of services (collectively, "Records") for five (5) years after the final payment made by WVOT. Confirm that Vendor's accounting procedures and practices conform to generally accepted accounting principles ("GAAP") and that the costs applicable to WVOT will be readily ascertainable from Vendor's Records.

3.12.10 **[Critical]** Audit Documentation: WVOT requires that the service provider submit to audits performed by the State Department of Audits and Accounts, an authorized entity, at any reasonable time during its normal business hours, to inspect and audit any Records. Confirm that Vendor will submit to such audits and that Vendor will deliver any required documentation and Records in preparation of such audits.

3.12.11 **[Critical]** All requests for service under this contract shall be submitted to the successful vendor by the WVOT, or a WVOT-authorized user, via a TCR. No service shall be installed by the successful vendor without a TCR that has been approved by WVOT. The vendor's failure to conform to this requirement may result in non-payment of services.

3.12.12 The Vendor should communicate electronically, at a minimum, once per week to WVOT, or a WVOT-authorized user, with the TCR number, the vendor's work order number, and the due date of installation for all TCRs received from WVOT. Vendor should state their willingness to comply with this request.

3.12.13 TCRs will not be required to be submitted by the State for the conversion of existing service. They will only be submitted when requesting new circuits, new features on existing circuits, etc. Vendor should confirm acceptance.

3.12.14 Escalation and reporting procedures for service outages should be provided by the successful vendor(s) prior to award. Escalation schedules shall contain escalation timeframes from point of incident and telephone numbers for all levels of activity on the escalation schedule. Trouble call management escalation may include high priority reporting and resolution centers and not necessarily individuals. The State requests that all this information be included with the vendor's response to the bid.

3.12.15 The Vendor should provide descriptions of outage classifications and describe how they will prioritize these outage classifications.

3.13 **Credits**

3.13.1 **[Critical]** Credits for Billing Errors: WVOT requires that credits for items billed in error or for other reasons should be refunded in the form of a credit against the monthly invoice. The credits should clearly identify which data circuit/voice lines are receiving the credit.

3.13.2 **[Critical]** WVOT requires all credits should be resolved within a maximum of three (3) billing cycles. Describe Vendor's approach. If the credit is not received within the three billing cycles, the WVOT reserves the right to deduct it from the amount due on the 4th billing cycle.

3.14 **Billing Escalation**

3.14.1 Billing Escalation: WVOT desires that the Service Provider establish and document a billing escalation process to resolve any billing issue including discrepancies, errors, omissions, or unrecognized charges. Describe Vendor's billing escalation process.

3.14.2 Tracking of all Billing Issues: Describe the process for tracking the status of all billing issues, inquiries, credits, refunds, and disputes.

3.15 Dispute Resolution Process

3.15.1 Dispute Resolution Process: Define billing dispute resolution process and benchmark timelines to resolve. Include WVOT responsibilities.

3.15.2 Dispute Resolution: WVOT desires that all disputes should be resolved within a maximum of three (3) billing cycles. Describe the approach to handling this request.

3.16 Transition and Acceptance

3.16.1 Project Management -Implementation

3.16.1.1 **[Critical]** The requirements of this section will be at no additional charge to the State, including, but not limited to, Travel, Lodging and Meals. All costs should be inclusive.

3.16.1.2 **[Critical]** Given the stringent implementation timeframes, the State is requiring the successful vendor(s) to assign an implementation team to ensure a smooth transition to the new network and vendor.

3.16.1.3 **[Critical]** Vendor shall submit, as part of their quote, an implementation plan that ensures the smooth transition to the new service.

3.16.1.4 Each member of the implementation team should be dedicated to this project and shall not be assigned any other projects without the written approval of the State.

3.16.1.5 **[Critical]** At a minimum, the implementation team shall include a Project Manager (who has worked on an implementation of this magnitude in the past 12 months) and a minimum of three implementation specialists (who have worked on an implementation of this magnitude in the past 12 months). All members of the implementation team should have a technical background in Telecommunications. The Project Manager shall be qualified and experienced in Project Management skills (PMI certification is desirable).

3.16.1.6 Vendors should provide qualifications, resumes and past experience for the people designated to be on the Implementation Team.

3.16.1.7 Vendors should provide a synopsis of similar work of this magnitude performed by the Implementation team within the past 12 months. (This request is in addition to mandatory vendor business references.)

3.16.1.8 There will need to be face-to-face discussions at different stages throughout the implementation phase. The implementation team should agree to have these meetings in Charleston, West Virginia, or at a location within West Virginia, as specified by the State.

3.16.1.9 There should be conference calls at least on a weekly basis with all members of the Implementation Team. The conference bridge for these conference calls should be provided by the vendor at no charge to the State.

3.16.1.10 **[Critical]** The Project Manager will be responsible for disseminating meeting minutes no later than the next business day after the conference call/face-to-face meeting. In addition to the meeting minutes, the Project Manager shall also be responsible for the creation and update of a timeline, which clearly shows the progress being made on the implementation of the different circuit types for the different entities.

3.16.1.11 On a weekly basis, the Project Manager should prepare an Executive Status Report, showing the progress made and activities planned for the upcoming week. **State the Vendor's ability to comply with each of the Project Management requirements individually.**

3.16.1.12 It is the State's desire that the Project Manager(s) and the Implementation Team(s) be housed at, or near, the WVOT's Facility in Charleston, WV during the implementation phase.

3.16.1.13 **[Critical]** WVOT would be responsible for providing only the office space and network connectivity and Internet connectivity required for the Implementation team members. All PC hardware, peripherals, etc. are the responsibility of the vendor. **Describe and clearly state the Vendor's ability to comply with this requirement.**

3.16.1.14 **[Critical]** Any VPN access that may be needed by the Implementation team to connect back to the corporate network will be the responsibility of the vendor. **Describe and clearly state the Vendor's ability to comply with this requirement.**

3.16.1.15 **[Critical]** Project Plan: Submit a representative, but detailed, project management plan that includes items such as: methodology, processes, procedures, WBS and schedule, demonstrating understanding of the scope and issues involved. The project plan is especially critical to the success of this effort. WVOT realizes that the sequence of cutovers for the approximately 2000 sites will have to be created in collaboration with the Service Provider. Different Agencies have critical business events at different times of the year, specifically K-12 and the Library Commission should be cut-over in a relatively short period of time and represent approximately 1500 sites. **Describe in detail how the vendor plans to meet or exceed the aforementioned requirements.**

3.16.2 **Design Plan**

3.16.2.1 **[Critical]** Design Plan: Vendor should provide a recommended design to include Access Circuits and CPE for each location. Vendors should view data circuits by geographic region on page 24 and also noted again in Appendix A.

3.16.3 **Access Circuits** Type of Access Circuit: For each general type of Access Circuit (DSL, ADSL, SDSL, Frame Relay T-1, T-1 Clear Channel, DS-3, OC-3, 10Mb Fast Ethernet, 100Mb Fast Ethernet and 1Gb Fast Ethernet), attach a project plan and schedule, for the transition of an example site and all other activities associated with the

transition. WVOT expects that the Service Provider will have inventory reconciliation. Describe the inventory reconciliation process. The project plan should address, at a minimum, the following areas:

- Billing
- Provisioning
- Training
- Installation
- Design
- Inventory Reconciliation
- Testing
- Acceptance
- Cutover
- Risk Management plan
- Change Order plan
- Escalation procedure

Assumptions on times to deal with other parties (agency site personnel, WVOT, local access providers, etc.)

3.16.4 **Staffing Plan**

3.16.4.1 Staffing Proposal: The Vendor should present a staffing proposal that illustrates the best mix of skills and experience to achieve project objectives.

3.16.4.2 Key Personnel: Describe and provide names, resumes and responsibilities of all Key Personnel (if any) and time commitments of proposed staff (full time/part time and/or number of man days/months/years/ per person over the course of the transition project. At a minimum, Vendor should include the Project Leader and the Technical Lead.

3.16.5 **Vendor Qualifications**

3.16.5.1 **[Critical]** Prior Project Experience: Identify four examples of prior like-size MPLS deployment projects of similar scope and magnitude in which Vendor performed transition and installation. It is highly desirable that the experience referenced above be a conversion from a State or Federal government entity that was using a frame relay/ATM environment connected via traditional Telco circuits like the State of West Virginia currently has in place to the fully meshed environment of MPLS VPN services.

3.16.5.2 **[Critical]** Customer References: Provide four (4) references of customers of like size (more than 1,000 sites), at least one (1) of which should be a governmental installation using an MPLS VPN network. References should describe in detail the type and duration of services, dates of service, and effectiveness of the services provided. Each reference will be evaluated for content and relevance. Vendor's reference information shall not exceed five pages in total for each reference. If the Vendor is partnering with a subcontractor, two separate references should be provided for the subcontractor in the same format defined in Appendix G – Corporate Reference Form. WVOT reserves the right to contact references, as well as develop its own references.

3.16.5.3 Organizational Chart: Provide an organizational chart for the personnel who will be providing deliverables and/or performing the services requested during the transition. Changes of Key Personnel during the transition are subject to WVOT approval. Such approval will not be unreasonably withheld.

3.16.5.4 Resources: Outline the Agency and WVOT resources that would be required to interface with the Service Provider and the amount of time necessary.

3.16.5.5 Staff Experience: Submit resumes with references for each proposed key staff member employed by either Vendor or subcontractor.

3.16.6 **Subcontractors**

3.16.6.1 Named Subcontractors: The Vendor should disclose the planned use of any subcontractor that will perform twenty percent or more of the services described in the RFP. In addition, Vendor may choose to identify any other subcontractor that Vendor believes may add value.

3.16.6.2 Named Subcontractor Information: Vendor should provide the following information: Name and address of each Named Subcontractor and the work the subcontractor will be performing.

3.16.6.3 Subcontractor Approval: Adding or changing Named Subcontractors during the contract should have prior WVOT approval.

3.16.6.4 **[Critical]** Subcontractor Performance: The Service Provider will be responsible for the performance of any subcontractors and will not be relieved by non-performance of any sub-contractors. Vendor shall provide a summary of qualifications, years of experience, and references for all Named Subcontractors.

3.16.7 **Timeline**

3.16.7.1 **[Critical]** All Sites: Propose a representative timeline for the transition of the approximately 1800 sites. It is not necessary to call out individual sites, but the Service Provider should provide justification for the proposed timeline.

3.16.7.2 **[Critical]** Liquidated Damages for Missed Timeline: Prior to award, WVOT and the apparent successful vendor/Service Provider will negotiate a mutually agreeable final timeline, based on the Vendor's proposed timeline. For each Access Circuit that is not transitioned more than fifteen (15) Business Days after the date set forth in the timeline due to delays not caused by WVOT or its Customers. Service Provider shall pay to WVOT, as liquidated damages, an amount equal to two (2) times the current MRC for such circuit. Thereafter, for each additional monthly billing period during which such Access Circuit is not transitioned due to delays not caused by WVOT or its Customers, the Service Provider shall pay WVOT an additional amount equal to two (2) times the current MRC for each such circuit. This requirement only applies to the circuits currently available from DATA05. This does not apply to the conversion of Voice/DAIN service, which has been exempted from this timeline.

3.16.8 **Technology Refresh**

Describe how a technology refresh, router upgrade, after hours (1800 – 0500) work and network maintenance would be accomplished during the transition.

3.16.9 **Cutover**

This is the time when testing of the circuit should be accomplished. WVOT requires that the Service Provider address the following:

3.16.9.1 **[Critical]** Cutover Methodology: Describe the methodology, processes, and procedures for the logical and physical cutover of the network.

3.16.9.2 **[Critical]** Cutover Backout: Describe the methodology, processes and procedures if the site conversion fails.

3.16.9.3 **[Critical]** Cutover Change Management: Describe the change management plan for transition.

3.16.9.4 **[Critical]** Cutover Test Plan: Describe the test plan for cutting over each site.

3.16.10 **Acceptance**

The acceptance of the circuits is to ensure that bandwidth, latency, and throughput have been provisioned successfully.

3.16.10.1 Acceptance Methodology of Service Provider: Describe the methodology, processes and procedures for acceptance after the transition has been completed.

3.16.10.2 **[Critical]** Default Acceptance: Absent mutual agreement between WVOT and the Service Provider, the acceptance process set forth in Section five (5) of the WVOT contract controls. The performance period shall begin on the installation date and shall end when the installed services have met the standard of performance for a period of thirty (30) consecutive days. The standard of performance shall be as proposed in the vendor's SLA. In the event the installed services do not meet the standard of performance during the initial thirty (30 consecutive days, the standard of performance test shall continue on a day-by-day basis until the standard of performance is met for a total of thirty (30) consecutive days. If the installed services does not meet the standard of performance after one hundred and twenty (120) calendar days, from the installation date, or the first day from the start of the performance period if such is delayed by the State, the State may at its option request to terminate the order and seek alternative plans.

3.16.10.3 Acceptance Reports: Describe and provide sample of the reports that are provided to ensure that, after the transition, the network is operating within specified parameters.

3.16.10.4 **[Critical]** Acceptance Billing: WVOT's obligation to pay shall begin only after WVOT accepts the service and the Service Provider issues a disconnect order for current service.

3.16.11 **Training**

Describe the initial training methodology that is provided for network management, ordering, billing, and problem management. (i.e. train the trainer, web- based, on customer site, etc.)

3.16.12 **Disentanglement**

WVOT expects full, complete, and timely cooperation in disentangling the relationship in the event that the Agreement expires or terminates for any reason. In the event of expiration or termination, WVOT expects that the Service Provider shall, among other things: return all State data and documentation to WVOT, including but not limited to configuration information; transfer ownership of all CPE at no cost to WVOT (other than the payments already received by Service Provider under the Agreement); and, allow WVOT or the replacement provider(s) continued access to all billing, ordering, and trouble ticketing systems, and processes that have been employed in servicing the State, in accordance with methods and procedures to be agreed upon and established in the Agreement. In the event of the expiration or termination of the relationship between WVOT and the Service Provider, the Service Provider shall:

3.16.12.1 **[Critical]** Disentanglement Approach and Process: The Vendor's Proposal should describe its specific approach to the Disentanglement process. Specifically, state the Vendor's proposed plan for Disentanglement, including key milestones and WVOT/ Service Provider roles and responsibilities. Provide time estimates for the Disentanglement process based upon the number of locations detailed in this RFP.

3.16.12.2 **[Critical]** Cooperation and Information: Service Provider is required to agree to cooperate with WVOT and/or the replacement provider(s) and otherwise take all reasonable steps to assist WVOT in effecting a smooth disentanglement upon the expiration or termination of the Agreement, including the provision of information necessary to enable the WVOT's personnel, or that of a replacement provider(s), to fully assume and continue without interruption the provision of Services. Vendor's proposal should state their understanding of this paragraph and provide any details, conditions or assumptions.

3.16.12.3 **[Critical]** Continued Service: Agree not to: (i) interrupt the provision of Services to WVOT and its Customers or any obligations related to disentanglement, (ii) disable any hardware used to provide Services, or (iii) perform any other action that prevents, slows down, or reduces in any way the provision of Services to WVOT or WVOT's Customers until WVOT agrees that a satisfactory disentanglement has occurred. Vendor's proposal should state their acknowledgement and agreement to each of the subparts of this paragraph and provide any details, conditions or assumptions.

Section 3.17 – Service Requirements & SLA(s)

3.17.1 Maintenance Requirements

[Critical] The successful vendor shall be responsible for the on-going maintenance of the MPLS Core and its Peripheral Edge Routers, Regional or Central

Office based Ethernet Switches and all other Peripheral Edge devices as well as all circuits and services such as Hosted Voice Services, even those that may utilize a third-party to provide the "last mile". The successful Vendor will also be responsible for maintaining adequate bandwidth on the MPLS core and Peripheral Edges as well as the ability to increase circuit size and CoS in all regions to ensure adequate potential for rapid expansion as described in the SLA you submit.

Scheduled maintenance should occur on Sunday mornings beginning no earlier than 2AM with completion no later than 6AM EST. Any maintenance that extends outside of these parameters will be included in the calculation for determining system availability (refer to Service Level Guarantee requirements for more detail).

Vendor should provide at least ten (10) calendar days advance notification, in writing (e-mail), to The Office of Technology's Help Desk and the Telecom Customer Service and Billing, (TCS&B), designee and or exempt Agency designee as assigned by the WVOT's TCS&B team's designee, of any scheduled maintenance. The WVOT will then disseminate.

In the event of required emergency maintenance, the vendor shall inform both the Help desk and appropriate WVOT TCS&B designee OR "as authorized" the Agency designee and receive verbal approval prior to working on the circuits or any infrastructure that may affect the traffic flowing across the MPLS and any and all circuits VPN(s), VRF(s) Etc. **State that the Vendor complies with our maintenance requirements as described above. This should also be written into each SLA section or SLA(s).**

3.17.2 Service Level Guarantee

The SLA's are broken into A: MPLS Core specific, B: Access Circuits, C: VoIP Services (meaning IP trunking and Hosted IP Voice Services) , and D: Internet Access, (If the Vendor offered Internet Access as an Option), all are defined in the sections following. The Vendor should address each section in the body of this RFP and include a response to the mandatories at a minimum and your comprehensive SLA/SLA(s) submitted as an attachment(s) to your RFP response. ***We strongly advise that the Vendor either respond with a primary SLA broken into three sections addressing A: MPLS Core Specific parameters, and a separate section addressing B: Access Circuits, and C: VoIP Services, and a separate Internet Services SLA, OR the Vendor responds with up to four separate SLA(s) for the three required SLA sections that need to be responded to and then possibly a forth SLA for D: Internet Services should said Vendor have offered an Internet Services offering in their RFP response.***

The State reserves the right to negotiate the most advantageous SLA(s) with the apparent winning Vendor who by definition should have met all minimum requirements of our SLA(s), however if the State cannot negotiate favorable SLA's and associated penalties for failure to comply with the negotiated SLA(s) then the State reserves the right to negotiate with the second best value Vendor for favorable SLA(s) and corresponding penalties for non-compliance. State your understanding and acceptance of the above.

Force Majeure. The State of WV recognizes any delay in or failure of performance by the vendor will not be considered a breach of any SLA if and to the extent caused by events beyond its reasonable control, including, but not limited to, acts of God,

embargoes, governmental restrictions, strikes, lockouts, work stoppages or other labor difficulties, riots, insurrection, wars, or other military action, acts of terrorism, civil disorders, rebellion, fires, floods, vandalism, or sabotage. No response necessary. However: we advise that the vendor to address in their attached SLA(s).

3.17.3 MPLS VPN Core Network :SLA "A", or Section "A" in single SLA

The Service Standards, provisions, and Remedies listed in this section refer to the Vendor's proposed MPLS VPN Network (MPLS domain), (CE to CE), section A, excluding Access Circuits. Remedies can include service credits, payments, or other consideration. Read and respond as directed. **No specific response is required here.**

Guarantees and Exclusions:

3.17.3.1 **[Critical]** Guarantees: The Vendor should offer, in the SLA, Service Standard guarantees for the MPLS VPN Core Network (MPLS domain). The guarantees should include Availability, Latency, Jitter, Packet Delivery, and Outage Notification. **State that the Vendor understands this mandatory and complies by addressing in your proposal's SLA.**

3.17.3.2 **[Critical]** Exclusions: With respect to calculating Availability, any exclusions for scheduled maintenance, time lost waiting for premises access, or other reasons should be clearly detailed in the Vendor's proposal.. **State Vendor's understanding of this mandatory and address clearly in the SLA.**

3.17.3.3 MPLS VPN (CE to CE) Network Minimum Service Standards Table: **Please confirm compliance here following the table and address in your SLA.**

Measure	Definition	Mandatory Service Standard
Availability	Percentage of time that the Vendor's MPLS VPN Network is available for use by WVOT and WVOT Customers. This is 100 – (outage minutes / monthly minutes). MPLS VPN Network outages are defined as a loss of ability to transmit IP packets, packet loss of 1% or more, or latency of 80 ms or greater on the MPLS VPN Network.	99.99%
Latency	Latency refers to the average time required (delay), in milliseconds, for one-way packet transmission from any Edge Router on the Vendor's MPLS VPN Network to any other Edge Router on the Vendor's MPLS VPN Network. Latency in Access Circuits is not included.	36 ms
Jitter	Jitter refers to the standard deviation of variation in Latency from packet to packet. For the purposes of this SLA, Jitter refers to transmissions across any portion of the Vendor's MPLS VPN Network, excluding Access Circuits.	< 5 ms
Packet Delivery	Packet Delivery is the proportion of packets transmitted from a sender that are received by the intended receiver.	99.5 %
Outage Notification Period	The Vendor will contact WVOT with notification of an outage within the Outage Notification Period for any service affecting outage.	15 minutes

111

Availability:

3.17.3.4 **[Critical]** Backbone Availability Required: It is required that the Vendor offer a Service Standard guarantee for Availability of the MPLS VPN Core Network of at least 99.99%, measured each month. MPLS VPN Core Network outages are defined as a loss of ability to transmit IP packets, packet loss of 1% or more, or latency of 80 ms or greater on the MPLS VPN Core Network. **Confirm Vendor's compliance with this mandatory and address in your SLA.**

3.17.3.5 Backbone Availability Preferred: It is desirable that the Vendor offer a Service Standard guarantee for Availability of at least 99.999% for the MPLS VPN Core Network. **State Vendor's understanding and address in your SLA submitted.**

3.17.3.6 **[Critical]** Backbone Availability Remedy: It is required that the Vendor offer a remedy for failure to meet a monthly Service Standard guarantee for Availability of the MPLS VPN Core Network. . **State Vendor's understanding and address in your SLA submitted.**

Latency:

3.17.3.7 **[Critical]** Backbone Latency Guarantee: It is required that the Vendor offer a Service Standard guarantee for one-way latency of 36 ms or less, measured across any portion of the Vendor's proposed MPLS VPN Core Network to any other, edge to edge, not including Access Circuits or CPE. **Confirm Vendor's compliance with this mandatory and address in your SLA.**

3.17.3.8 Backbone Latency Remedy: It is desired that the Vendor offer a remedy for failure to meet a monthly Service Standard guarantee for Latency on the MPLS VPN Core Network. . **State Vendor's understanding and address in your SLA submitted.**

Jitter:

3.17.3.9 **[Critical]** Backbone Jitter: The Vendor should offer a Service Standard guarantee of a minimum of five (5) ms for Jitter across any part of the Vendor's MPLS VPN Core Network. **Confirm Vendor's compliance with this mandatory and address in your SLA.**

3.17.3.10 Preferred Backbone Jitter: It is preferred that the Vendor offer a Service Standard Guarantee of better than five (5) ms for Jitter across any part of the Vendor's MPLS VPN Core Network. This excludes Access Circuits. **State Vendor's' base price for the MPLS VPN Core backbone jitter, in ms.**

3.17.3.11 Backbone Jitter Remedy: It is desired that the Vendor offer a remedy for failure to meet a monthly Service Standard guarantee for Jitter on the MPLS VPN Core Network. **State Vendor's understanding and address in your SLA submitted.**

Packet Delivery:

3.17.3.12 **[Critical]** Backbone Packet Delivery: It is required that the Vendor offer a Service Standard guarantee for Packet Delivery of 99.5 % with respect to the MPLS

VPN Core Network, from sender to receiver. **Confirm Vendor's compliance with this mandatory and address in your SLA.**

3.17.3.13 Preferred Backbone Packet Delivery: It is preferred that the Vendor offer a Service Standard guarantee for Packet Delivery of 99.9% with respect to the MPLS VPN Core Network proposed. **State Vendor's understanding and address in your SLA submitted.**

3.17.3.14 Backbone Packet Delivery Remedy: It is desired that the Vendor offer a remedy for failure to meet a monthly Service Standard guarantee for Packet Delivery on the MPLS VPN Core Network. **State Vendor's understanding and address in your SLA submitted.**

Outage Notification:

3.17.3.15 **[Critical]** Outage Notification: It is required that the Vendor provide a Service Standard guarantee of 15 minutes for notifying WVOT's Network Operation Center (NOC/Help Desk) by telephone of any service affecting outage on the MPLS VPN Core Network. These outages are defined as a loss of ability to transmit IP packets, packet loss of 1% or more, or latency of 80 ms or greater on the MPLS VPN Core Network. **State Vendor's understanding and address in your SLA submitted.**

3.17.3.16 Preferred Outage Notification: It is preferred that the Vendor offer a Service Standard of 5 minutes for service affecting outages on the MPLS VPN Core Network. **State Vendor's understanding and address in your SLA submitted.**

3.17.3.17 Backbone Outage Notification Remedy: It is desired that the Vendor offer a remedy for failure to meet a monthly Service Standard guarantee for Outage Notification with respect to the MPLS VPN Core Network. **State Vendor's understanding and address in your SLA submitted.**

Additional Guarantees and Provisions:

3.17.3.18 Additional Guarantees: It is desirable that the Vendor offer additional Service Standard guarantees, provisions, and remedies with respect to the Vendor's MPLS VPN Core Network. These might include such measures as Mean Time to Repair (MTTR) or Maximum Service Affecting Outage Duration. **State Vendor's understanding and address in your SLA submitted.**

3.17.3.19 Chronic Outages and Missed Service Standards: The Vendor should offer provisions and remedies for chronic outages and chronic missed Service Standards. **State Vendor's understanding and address in your SLA submitted. Outages**

3.17.3.20 **[Critical]** The vendor should describe, in detail, their levels of service guarantee and remedies for outages ***in all of the SLA(s) or the appropriate section of the SLA or SLA(s) they are required to provide.*** The vendor's response should meet or exceed the minimum expectations required by the State of West Virginia's Public Service Commission (PSC). If a vendor fails to describe their service level or does not meet the PSC requirements, the State reserves the right to require the vendor to provide any information within one (1) business day. Failure on the vendor's part to provide this information may result in the vendor's quote to be disqualified from

further evaluation. Any costs associated with the different levels of service guarantee should be identified in the Cost Proposal. The minimum guaranteed expectations required by the State of WV Public Service Commission **should** be included in the cost of the Access Circuits and base MPLS proposal at no additional costs. If higher levels of service guarantees' may be offered in the SLA and listed separately and clearly labeled in the optional cost in Appendix E. **State the Vendor's ability to comply with this Mandatory (minimum response time for outages as stipulated by the PSC), and elaborate and offer an' additional and stronger service guarantees in your SLA noting if there is a cost for such. However, only put the cost if it applies in Appendix E. The Vendor is cautioned to be explicitly clear in their response to outages, and service guarantee and resulting remedies of the base minimum required as stated above, which by definition comes with the base price in the SLA, (no additional charge).**

3.17.4 **Access Circuits Availability: SLA, B or Section B in single SLA**

3.17.4.1 Availability is the total number of Hard Outage minutes in a calendar month for a specific State Connection, divided by the total number of minutes in a calendar month. Availability is comprised of the State's Access Router to the Vendor's MPLS Access to the core router. **State that the Vendor understands our definition and will comply with and address in this section of the SLA:**

3.17.4.2 **[Critical]** Access Circuit Availability: It is required that the Vendor offer a Service Standard of 99.9% for access circuits. **Confirm Vendor's compliance with this mandatory and address in your SLA**

3.17.4.3 **Calculation.** Availability is calculated once an alert or notification is received by the NOC, and is determined by the percentage of time that the Connection is available within a given calendar month. Monthly Network Availability (%) =: **State that the Vendor agrees with and understands our definition and address in your SLA and clearly define whether or not scheduled maintenance is excluded from time factors.**

$$1 - \left(\frac{\text{Total minutes of connection outage per month}}{\text{Days in month x 24 hours x 60 minutes}} \right) \times 100$$

3.17.4.4 **Credit Structure**. The credit is based on the number of minutes of down time independent of the actual percent availability calculation. The following tables contain the percentage availability translated into minutes of up time and downtime for the SLA. **State that the Vendor understands our credit structure scoring and will comply in their SLA with our definition and formula for credit structuring and that they will address in their SLA, as applicable.**

Total Minutes In A Given Calendar Month	
Month in Days	**Total Minutes**
31 Day Month	44,640
30 Day Month	43,200
29 Day Month	41,760
28 Day Month	40,320

Availability % Translated to Minutes Up and Minutes Down		
Percentage by Days per Month	**Minutes Up**	**Minutes Down**
99.9% for 31 days	44,595	45
99.9% for 30 Days	43,157	43
99.9% for 29 Days	41,718	42
99.9% for 28 Days	40,280	40

Note: No SLA's apply to sites using DSL connectivity as the access methodology

Any Access circuit that falls below the 99.9% access circuit guarantee will receive a full Monthly Recurring Access Cost from the vendor for that location. **State Vendor's acceptance of this requirement and address in your SLA.**

3.17.5 VoIP SLA or Section C in single SLA

3.17.5.1 Overview: The Vendor should support quality service on Voice over IP ("VoIP") by offering a performance Service Level Agreement (SLA) to the State for all locations that implement VoIP service using Internet Dedicated, or the MPLS transport services. The VoIP SLA is in lieu of, and takes precedence for VoIP users in each affected area, any other SLAs for Internet Dedicated service, or the MPLS. Performance standards in the SLA cover: Jitter, Latency, Packet Delivery, and Network Availability. **State the Vendor's acceptance of this requirement and address your understanding and compliance in your VoIP Services, C: SLA.**

3.17.5.2 VoIP Jitter Service Level Agreement: Also known as delay variation, jitter is defined as the variation or difference in the end-to-end delay between received packets of an IP or packet stream. Jitter is usually caused by imperfections in hardware or software optimization or varying traffic conditions and loading. Excessive delay variation in packet streams usually results in additional packet loss which impacts voice quality. **State the Vendor's acceptance and understanding of this definition.**

3.17.5.2.1 **[Critical]** The VoIP Jitter SLA requires that the vendor's contiguous Network monthly jitter performance will not exceed 1.0 millisecond between the transit backbone network routers ("Hub Routers"). **State the Vendor's acceptance of this Mandatory and address in your SLA.**

3.17.5.3 **[Critical]** Network Latency Service Level Agreement: The VoIP Latency SLA should provide that the Vendor's Network Latency performance will have a monthly average **round-trip transmission** of fifty-five (55) milliseconds or less between the backbone network routers provided by the vendor for access into the VoIP services. **State Vendor's acceptance of this Mandatory and address in your SLA.**

3.17.5.4 **[Critical]** Network Packet Delivery Service Level Agreement: The VoIP Packet Delivery SLA provides that the Vendor's monthly packet delivery rate will be 99.5 percent or greater for data delivery between the backbone network routers ("Hub

115

Routers"). **State Vendor's acceptance of this Mandatory and address in your SLA.**

3.17.5.5 **[Critical]** Network Availability Service Level Agreement: The VoIP Network Availability SLA should provide that the Vendor's Network will be available at least 99.9 percent of the time as measured on a monthly basis by trouble ticket time. The Network is considered not available for the number of minutes that a trouble ticket shows the Network was not available to the State of West Virginia. The unavailable time is started when the State opens a trouble ticket with the Customer Support Center. The unavailable time stops when the applicable Network or access circuit trouble has been resolved and the service is again available to the State. This should be measured in a proactive manner. Please describe your proactive capabilities.

With the exceptions noted below: State the Vendor's ability to comply with this mandatory and address in section C of your SLA or SLA C.

This will not include unavailability resulting from:

- Network maintenance;
- Third-party circuits;
- Inappropriate State configuration change(s)
- State owned Premise Equipment including, but not limited to, State provided PBX, black phones, SIP phones, Quality of Service Box, firewalls, Router/modem and/or Analog/Ethernet Adapter;
- Acts or omissions of the State, or any use or user of the service that is authorized by State but outside the scope of State's service;
- Reasons of Force Majeure (as defined in the applicable underlying Service Level Guarantee).

3.17.6 Internet Access SLA (Optional: Dependent upon Vendor's response to the optional request for Internet service)

3.17.6.1 Availability: Service Availability SLA Scope. The Internet Provider's Service Level Agreement (SLA) should provide that the Internet access provided to the MPLS core will be available 99.99% of the time. The State of West Virginia should be credited for the pro-rated charges for one day of the Monthly Fee when the network availability falls below 99.99%. **State the Vendor's willingness to comply with this desirable and address in SLA D.**

3.17.6.2 Latency: Latency SLA Scope. The vendor's Latency SLA should provide for an average round-trip transmission of 55 milliseconds or less between provider's Internet access ports and their inter-regional transit backbone routers ("Hub Routers") in the contiguous U.S. The State of West Virginia should be credited for the pro-rated charges for one day of the Monthly Fee when Latency exceeds 55 milliseconds. **State the Vendor's willingness to comply with this desirable and address in SLA D.**

3.17.6.3 Network Packet Delivery Network Packet Delivery SLA Scope. The vendor should offer a provision for both a North American, and a Transatlantic Network

Packet Delivery SLA. The North American and Transatlantic Network Packet Delivery SLA should provide for a monthly packet delivery of 99.5% or greater between the access point at the MPLS core and the Hub Routers in North America. If the vendor's Packet Delivery SLA in a calendar month is not met the State of West Virginia should be credited for the Internet Access charges for that month. **State the Vendor's willingness to comply with this desirable and address in SLA D.**

3.17.6.4 Denial of Service SLA Scope. The vendor will respond to Denial of Service attacks reported by the State within 15 minutes of the State opening a complete trouble ticket with the WVOT Service Desk. The State defines a Denial of Service attack as more than 95% bandwidth utilization. The State of West Virginia should be credit for the pro-rated charges for one day of the Monthly Fee when the vendor fails to respond to a Denial of Service attach that has been reported by the State of West Virginia. **State the Vendor's willingness to comply with this desirable and address in SLA D.**

3.17.6.5 SLA Scope – Network Outage: The Network Outage SLA should provide the State of West Virginia notification within 15 minutes after it is determined that Service is unavailable. The standard procedure will be to ping the State's router every five minutes. If the router does not respond after two consecutive five-minute ping cycles, the vendor will deem the Service unavailable and the State of West Virginia's point of contact will be notified by e-mail, phone or pager. **State the Vendor's willingness to comply with this desirable and address in SLA D.**

3.17.6.6 SLA Scope - Scheduled Maintenance: Scheduled Maintenance shall mean any maintenance that the vendor performs related to the State of West Virginia's Internet Access. The vendor should notify the State seven calendar days in advance. Notice of Scheduled Maintenance will be provided to the State's designated point of contact by email or pager. Upon receiving such notice, the State may request to have such maintenance postponed to a later date if agreed upon by the vendor and the State. **State the Vendor's willingness to comply with this desirable and address in SLA D.**

3.17.6.7 Network Jitter SLA Scope: Also known as delay variation, Jitter is defined as the variation or difference in the end-to-end delay between received packets of an IP or packet stream. Jitter is usually caused by imperfections in hardware or software optimization and varying traffic conditions and loading. Excessive delay variation in packet streams usually results in additional packet loss, which affects quality. The vendor's Network jitter performance will not exceed 1 millisecond. **State the Vendor's willingness to comply with this desirable and address in SLA D.**

3.18 **Pricing (Both Mandatory and Optional)**

3.18.1 **Overview**

The first component of the pricing section is Appendix B, which is comprised of three (3) charts which should be completed, in their entirety. Each chart has a score associated with it, totaling thirty (30) points. **This is the only section which counts toward the pricing score.**

The three charts making up Appendix B are pre-programmed to do the calculations across the rows and down the columns. When you type in the unit pricing, the

spreadsheet calculations will be automatic. If the columns don't show a total, it means that you have missed a row. Please double check your numbers before submitting your bid.

There are two (2) additional pricing sections which may be filled out, provided the Vendor offers options for Alternative Access Circuit types in Appendix C. The pricing for these options should be listed in Appendix D, and should correspond precisely with the offerings in Appendix C. **NO PRICING SHOULD APPEAR IN APPENDIX C, WHICH WILL BE PART OF THE TECHNICAL EVALUATION PORTION OF THIS RFP.**

The final pricing component of this RFP should be listed by Section number, and shall be comprised of the prices for WVOT requested optional services, provided by the Vendor, if applicable. The Vendor may provide information in the body of the RFP response, with respect to potential optional services, but should provide pricing for these services in Appendix E, utilizing the Section number references from the body of the RFP. This requirement is essential if the Vendor wishes the State to incorporate or include the aforementioned optional services into the final contract award. (Per State Purchasing guidelines, the State is under no obligation to make any award, in part or in whole, from the release of this RFP.)

3.18.1.1 Pricing Consistency: Where WVOT requests pricing information in more than one place or more than one price workbook, WVOT requires that Vendor's stated pricing for such items or components should be the same or consistent in all locations. Please confirm and explain. Failure to provide consistency may result in reduction of evaluation scoring.

3.18.2 End to End **[Critical]** Inclusive Pricing: Submit pricing that is all-inclusive of costs end to end and covers the costs of the MPLS core and Peripheral Edge equipment via the aggregate price of the access circuits as listed in Appendix B. The State realizes that any options provided may be additional and if the vendor wishes for the options provided to be purchased from the MPLS and Associated Services contract, those costs SHOULD be provided in the appropriate Appendices (D or E) as applicable. Confirm Vendor's compliance with this mandatory.

3.18.3 **Fixed Pricing**

Fixed Pricing: WVOT requires that all prices be fixed during each one-year term of the Contract. The vendor will be expected to pass through any price decreases at the time the price decrease is announced.

3.18.4 **Competitive Rates**

3.18.4.1 **[Critical]** Rates: WVOT requires that the pricing, rates and terms offered to WVOT during each one-year term of the Contract are at least as favorable as the pricing, rates and terms offered to Vendor's similarly situated customers. Describe Vendor's approach for keeping WVOT's pricing, rates and terms at least as favorable as those offered to Vendor's other customers.

3.18.4.2 **[Critical]** Competitive Market: WVOT requires that the pricing, rates

and terms offered to WVOT during each one-year term of the Contract remains competitive with the pricing, rates and terms offered in the market. Describe how Vendor will keep pricing, rates and terms competitive.

3.19 **Special Terms and Conditions:**

3.19.1 Bid and Performance Bonds: Vendor will provide a bid bond in the amount of the bid that will be held by the Division of Purchasing until the award is made. A performance bond may be required upon award, the amount of which will be made during contract negotiations.

3.19.2 Insurance Requirements: If applicable, the vendor will provide liability insurance according to State requirements. Insurance certificates are required prior to award but are not required at the time of bid.

3.19.3 License Requirements: The vendor will be responsible for obtaining Workers Compensation, a Contractor's License, etc. in compliance with the laws of the State of West Virginia.

3.19.4 Litigation Bond: Each bidder responding to this request for proposal **should** submit a litigation bond in the amount of $500,000, made payable to the State of West Virginia Purchasing Division. This bond should be issued by a surety company licensed to do business in the State of West Virginia with the West Virginia Insurance Commission, on a form acceptable to the State. The only acceptable alternate forms of the bond are (1) a company certified check (not an individual) and (2) a cashier's check.

The purpose of the litigation bond is to discourage unwarranted or frivolous law suits pertaining to the award of a contract from this request for proposal. Secondly, the bond provides a mechanism for the State of West Virginia, the Agency, it's officers, employees, or agents thereof to recover damages, including (but not limited to) attorney fees, loss of revenue, loss of grants or portions thereof, penalties imposed by the federal government and travel expenses which may result from any such litigation. A claim against the bond will be made if the vendor contests the award in a court of competent jurisdiction and the grounds are found to be unwarranted or frivolous based on the facts of the award or applicable law as determined by the court.

Failure to submit an appropriate bond, or alternate bond with the proposal at the time of bid opening, constitutes a binding agreement between the vendor and the State, indicating that the vendor waives all rights of protest, including, but not limited to: competitor's bids, the evaluation of the bid responses, and the contract award to the apparent successful vendor.

The bond or alternate form should remain in effect for two years from the proposal submission date. After six (6) months, each vendor may request, and the State anticipates granting, a release of the litigation bond. However, the vendor will be required to provide a release (signed and notarized in a form that is acceptable to the State) prior to release of the bond which states that the vendor will not sue.

PART 4 PROPOSAL FORMAT

4.1 Vendor's Proposal Format:

The proposal should be formatted in the same order, providing the information listed below:

Title page - Should state the RFP Subject and number, the name of the Vendor, Vendor's business address, telephone number, name of authorized contact person to speak on behalf of the Vendor, that contact's e-mail address, business telephone number, and cell phone number. This title page should be dated and signed.

Table of Contents - Clearly identify the material by section and page number.

Section I - This section will address the Vendor's technical offering - responses to 3.1 (MPLS VPN Design Requirements) and 3.2 (MPLS VPN Management and Monitoring).

Section II – This section will address the Vendor's processes in supporting the State's account - responses to 3.3 (Trouble Ticketing), 3.4 (Reporting), 3.5 (Service Ordering), 3.6 (Service Provider's Help Desk and Network Operations Center), 3.7 (Moves, Adds, Changes and Deletions), and 3.8 (Change Orders).

Section III – This section will address the Vendor's processes in billing the State Account – responses to 3.9 (Contract Management and Billing Requirements), 3.10 (Billing), 3.11 (Billing Cycle), 3.12 (Invoice Presentation), 3.13 (Credits), 3.14 (Billing Escalation, and 3.15 (Dispute Resolution Process).

Section IV – This section will address the Vendor's plans for project management, vendor experience, and timelines, as well as the reference forms – responses to 3.16 (Transition and Acceptance). In addition, the vendor should include in this section his four positive like-size MPLS deployments as requested in Part 2, last paragraph of 2.2, using the vendor reference forms included as Appendix F.

Section V – The section will address what should be contained in the Vendor's submittals for the SLA requirements – responses to Section 3.17 (Service Requirements & SLA(s) for both the MPLS VPN Core and the VoIP Services on the MPLS VPN and the optional Internet Access SLA). The vendor should provide any SLA's submitted by the vendor. Only three SLAs, the MPLS Core/General, Access Circuits and the VOIP on the MPLS are required. The Internet Access SLA is only required if the responding vendor submits an option, or options, for Internet access. NOTE: The State reserves the right to further negotiate the SLA(s) with the apparent best value vendor. If the State cannot successfully negotiate the SLA(s) with the first apparent best value vendor, then the State reserves the right to cancel the award to the initial apparent best value vendor and begin negotiations with the second best value vendor.

Section VI – This section will include Appendix C, the description of alternative access circuits provided by the vendor in addition to those in Appendix B.

Section VII - This section will include all Cost Sheets (Exhibits B, D, and E). **(Please remember, the cost section SHOULD be included under separate cover)**

If applicable, sign and submit the attached Resident Vendor Preference Certificate with the proposal.

4.2 **Evaluation Process:**

4.2.1 Method of Evaluation:

The proposals will be evaluated by a committee of three (3) or more individuals in accordance with the criteria stated. The Vendor who meets all the mandatory specifications and attains the final highest point score of all vendors (possible one-hundred 100 points maximum) shall be awarded the contract. The selection of the successful vendor will be made by a consensus of the evaluation committee.

4.3 **Evaluation Criteria**: The following are the evaluation factors and maximum points possible for technical point scores:

A.	MPLS Core Requirements	15 Points Possible
B.	Portfolio of Optional Services	15 Points Possible
C.	Account Support	15 Points Possible
D.	Vendor Experience/References	15 Points Possible
E.	Service Level Agreements	10 Points Possible
F.	Cost	30 Points Possible
	Total	100 Points Possible

Each cost proposal cost will be evaluated by use of the following formula for all vendors who attained the Minimum acceptable score only:

$$\frac{\text{Lowest price of all proposals}}{\text{Price of Proposal being evaluated}} \times 30 = \text{Price Score}$$

The Price Scores of the three Pricing Charts will be totaled and those points added to each vendor's technical evaluation.

4.4 **Minimum Acceptable Score:**

Vendors should score a minimum of 70% of the total technical points possible (if doing oral presentation may require it for technical criteria not including the oral, in order to avoid interviewing non-qualified vendors). The minimum qualifying score would be 70% of 70 points or a technical score of 49 points or greater to be eligible for further consideration and to continue in the evaluation process. All vendors not attaining the minimum acceptable score (MAS) shall be disqualified and removed from further consideration.

The State will select the successful vendor's proposal based on best value purchasing which is not necessarily the low bidder. Cost is considered but is not the sole determining factor for award. The State does reserves the right to accept or reject any or all of the proposals, in whole or in part, without prejudice if to do so is felt to be in the best interests of the State.

Vendor's failure to provide complete and accurate information may be considered grounds for disqualification. The State reserves the right if necessary to ask vendors for additional information to clarify their proposals. Nothing may be added to alter the

written solution or method contained in the original proposal after the bid opening.

4.5. Cost Proposal Format/Pricing Charts

Each item listed in the Pricing Charts is a critical requirement from the RFP technical portion and is described in detail in the RFP.

The State in no way promises that we will purchase these anticipated volumes. They are strictly our best guess utilized to evaluate a representative monthly price for the purposes of determining the low cost vendor.

These pricing charts do not include the 1,474 State of WV Lottery 2.4 DDS Multi-drop circuits, but it is entirely possible that the Lottery will want to utilize the MPLS contract with their anticipated migration to IP.

The Vendor's Cost Proposal will be made up of the following:

Appendix B - Price Comparison Chart 1: A Unit Price Comparison by Circuit Access type and two Cost of Service Scenarios – worth 8 points

Appendix B - Price Comparison Chart 2: Projected Volumes that we estimate will be required one year after initial implementation – worth 14 points

Appendix B - Price Comparison Chart 3: Project Volumes that we estimate will be required three years after initial implementation – worth 8 points.

Appendix B - Summary of Worksheets: This is a sheet showing the totals from each of the above charts with a grand total. This grand total will be the basis for selecting the low cost vendor.

These estimates are representative of best known numbers and does not include many Metropolitan area Ethernet transport circuits as it is unlikely that the MPLS postalized circuit pricing, (i.e., all circuits of a particular Access type, speed {cir or port size depending on access type} and CoS), will be as low or cost effective as these exiting non-Data05 contract Metropolitan area circuits. However, it is important to note if a State agency wishes to connect to the MPLS or the State Internet service, they will be charged a port charge depending on the speed and QoS required by either the State of WV or the winning MPLS vendor.

The three charts making up Appendix B are pre-programmed to do the calculations across the rows and down the columns. When you type in the unit pricing, the spreadsheet calculations will be automatic. If the columns don't show a total, it means that you have missed a row. Please double check your numbers before submitting your bid.

Appendix D – Pricing for Alternative Access Offerings: The vendor may provide alternative access circuit types – the descriptions will be provided in Appendix C and the cost of these circuit types will be provided in Appendix D. No points will be associated with these costs although the vendor may receive technical points from the descriptions of these circuit types in Appendix C. If the State chooses, these items may be included in the offerings in the contract.

Appendix E – Pricing for Optional Services: The vendor may provide pricing for any optional services described in the RFP response. No points will be associated with these costs. If the vendor wishes to have their options considered to be included in the contract award, they must describe the option in the body of the RFP, and also separately provide pricing in this Appendix E clearly showing the RFP section where the option is described.

APPENDIX A – WEST VIRGINIA VOICE, VIDEO AND DATA ACCESS TYPES (APPROXIMATION OF THE CURRENT STATE ENVIRONMENT

The Circuit quantities provided below are an intelligent estimate of what will be cut over year one from 6/30/07 to 6/30/09, although the bulk of data circuits will be cut over by 6/30/08. We are uncertain as to the quantity of Ethernet facilities and Host IP Voice Services/IPTrunks that will be added or cutover.

TYPE OF CIRCUIT	QTY	LATA240	LATA256	LATA254	LATA932
PRI – Voice 23B+D/24B	130	25	35	60	10
Transport ADSL	175	40	55	60	20
Transport SDSL	50	10	15	20	5
T-1 Clear Channel	10	2	3	3	2
FR T-1 768cir burst to full T-1	1500	350	375	580	195
DS-0 FR 56K 28Kbps min cir	250	50	75	85	40
DS-0 Clear Channel	10	2	3	3	2
Centrex	7000	1165	1600	3600	635
Centrex with Voicemail	5000	700	1100	2900	300
Switched Ethernet 10 Meg	0	0	0	0	0
Switched Ethernet 10 Meg redundant local loop	0	0	0	0	0
Switched OC-3	0	0	0	0	0
Switched OC-3 redundant local loop/true Sonnet ring	0	0	0	0	0
Switched Ethernet 1 Gigabit	0	0	0	0	0
Switched Ethernet 1 Gigabit redundant local loop	0	0	0	0	0

NOTE: The State has approximately 25 to 35 metro area point-to-point Ethernet circuits which are not directly connected to the backbone as earlier described. The Ethernet circuits above would be connected to Ethernet switches at Points of Presence for the Vendor's MPLS Network.

APPENDIX B – MANDATORY PRICING TABLES AND INSTRUCTIONS (THIS APPENDIX, TOGETHER WITH APPENDICES D AND E, SHOULD BE SEPARATED FROM THE TECHNICAL PORTION OF VENDOR RESPONSES AND BE INCLUDED IN VENDOR'S SEALED, COST PORTION OF THEIR RESPONSE TO THIS RFP.)

These are provided as an attachment.

APPENDIX C – ALTERNATIVE ACCESS OFFERINGS (ACCESS CIRCUITS, WIRELESS, IP-TRUNKING/HOSTED VOICE SERVICES)

If the Vendor is offering alternative access circuit types, the technical specifications for those options should be provided in this Appendix. **NOTE: This Appendix should be included with your technical response, separate from Appendices which contain cost information. NO costs may appear in this Appendix – Appendix C is where you describe your alternative access offerings and Appendix D is where you should quote the costs for these offerings.**

PAGE# AND/OR RFP SECTION	DESCRIPTION OF OFFERING

APPENDIX D - ALTERNATIVE ACCESS OFFERINGS PRICING (THIS APPENDIX, TOGETHER WITH APPENDICES B AND E, SHOULD BE SEPARATED FROM THE TECHNICAL PORTION OF VENDOR RESPONSES AND BE INCLUDED IN VENDOR'S SEALED, COST PORTION OF THEIR RESPONSE TO THIS RFP.)

DESCRIPTION OF OFFERING	PAGE # AND/OR RFP SECTION	UNIT COST

APPENDIX E – PRICING FOR ALL VENDOR-PROVIDE OPTIONS

This appendix should provide pricing for any options that have an additional cost associated with them, as listed in the body of the technical response. (THIS APPENDIX, TOGETHER WITH APPENDICES B AND D, SHOULD BE SEPARATED FROM THE TECHNICAL PORTION OF VENDOR RESPONSES AND BE INCLUDED IN VENDOR'S SEALED, COST PORTION OF THEIR RESPONSE TO THIS RFP.)

DESCRIPTION OF OFFERING	PAGE# AND/OR RFP SECTION	UNIT COST

APPENDIX F- VENDOR REFERENCES

The vendor shall provide a minimum of three client references. The references shall be for systems of similar configuration. One of these references shall be for a system implementation in a similar, government facility environment.

Reference #1	
Company/Agency	
Contact Name	
Telephone Number	
E-mail Address	
Mailing Address	

Please provide a description of the system installed including general topology, software, hardware, number of users, etc. In particular, we want a description of the number of core MPLS routers, peripheral edge routers, and the number and type of circuit access terminations. In addition, we want to know what class of services does each VRF, VPN, and PVC have and whether the service is managed to the PE or to the customer premise.

Reference #2	
Company/Agency	
Contact Name	
Telephone Number	
E-mail Address	
Mailing Address	

Please provide a description of the system installed including general topology, software, hardware, number of users, etc. In particular, we want a description of the number of core MPLS routers, peripheral edge routers, and the number and type of circuit access terminations. In addition, we want to know what class of services does each VRF, VPN, and PVC have and whether the service is managed to the PE or to the customer premise.

Reference #3	
Company/Agency	
Contact Name	
Telephone Number	
E-mail Address	
Mailing Address	

Please provide a description of the system installed including general topology, software, hardware, number of users, etc. In particular, we want a description of the number of core MPLS routers, peripheral edge routers, and the number and type of circuit access terminations. In addition, we want to know what class of services does each VRF, VPN, and PVC have and whether the service is managed to the PE or to the customer premise.

131

Reference #4	
Company/Agency	
Contact Name	
Telephone Number	
E-mail Address	
Mailing Address	

Please provide a description of the system installed including general topology, software, hardware, number of users, etc. In particular, we want a description of the number of core MPLS routers, peripheral edge routers, and the number and type of circuit access terminations. In addition, we want to know what class of services does each VRF, VPN, and PVC have and whether the service is managed to the PE or to the customer premise.

State of West Virginia
Request for Proposal

Summary of Worksheets
Bidder:
0

	Third Party NRC	NRC Spread	Monthly Port Access	Annual Port Access	MPLS Carrier NRC	NRC Spread	$ Unit Cost/month and or minute *	Total monthly cost	Total Annual Cost
Price Comparison Chart 1	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Price Comparison Chart 2	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Price Comparison Chart 3	0	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Total	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00

AFFIDAVIT

West Virginia Code §5A-3-10a states:
No contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and the debt owned is an amount greater than one thousand dollars in the aggregate

DEFINITIONS:
"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Debtor" means any individual, corporation, partnership, association, limited liability company or any other form or business association owing a debt to the state or any of its political subdivisions. "Political subdivision" means any county commission; municipality; county board of education; any instrumentality established by a county or municipality; any separate corporation or instrumentality established by one or more counties or municipalities, as permitted by law; or any public body charged by law with the performance of a government function or whose jurisdiction is coextensive with one or more counties or municipalities. "Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

EXCEPTION:
The prohibition of this section does not apply where a vendor has contested any tax administered pursuant to chapter eleven of this code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

LICENSING:
Vendors must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agencies or political subdivision. Furthermore, the vendor must provide all necessary releases to obtain information to enable the Director or spending unit to verify that the vendor is licensed and in good standing with the above entities.

CONFIDENTIALITY:
The vendor agrees that he or she will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the agency's policies, procedures and rules. Vendors should visit **www.state.wv.us/admin/purchase/privacy** for the Notice of Agency Confidentiality Policies.

Under penalty of law for false swearing (West Virginia Code, §61-5-3), it is hereby certified that the vendor acknowledges the information in this said affidavit and are in compliance with the requirements as stated.

Vendor's Name: _____

Authorized Signature: _____ Date: _____