ADDENDUM

MANAGED INTERNET SERVICES RFP #29-2011,

LAMAR CONSOLIDATED ISD

TO: All Vendors

FROM: Lamar Consolidated ISD, Purchasing Dept.

DATE: November 22, 2011

RE: Addendum #2, RFP #29-2011

RFP# 29-2011, Managed Internet Services Questions and Responses

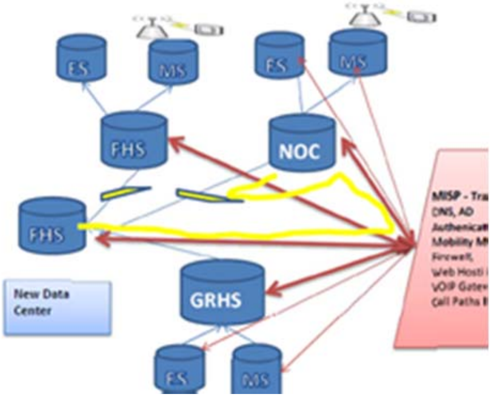
The following question and answer response addendum is a compilation of clarification questions submitted via email.

1. 5 year contract on #29-2011?
   a. 3 Year
2. Are P2P Circuits required to the aggregation points or could the solution be provided by a district wide MPLS network and allow Layer 3 routing to handle best Internet for each location.
   a. No, P2P are not required.
3. Section 3.3, metro E is by definition and design a shared network. MPLS provides isolated VRF table to each customer. Is a MPLS transport network required?
   a. No, MPLS is not required. The reference to “a secured, private network” is to describe the requirement that the network has no public access, the network only transports LCISD traffic and does not use the public Internet for transport.
4. In Section 3.3, does ‘’multi-connected Tier 1”” mean that simple peering points is unacceptable? Does this mean the selected provided must have multiple dedicated circuits to multiple Tier 1 providers?
   a. The respondent is not required to be a Tier 1 Internet provider. The respondent should provide a description of the proposed Internet design. The service provider’s network design will be evaluated as part of the evaluation.
5. Since the District desires AD authentication and security, is the District going to displace the Cisco ASA’s?
   a. The proposal should identify any equipment required or not required in the response.
6. Section 3.3:5; is this requesting management of external VPN’s? What encryption method is desired? (IPSEC, SSH, SST, SSL)
   a. This request is to manage the District’s cellular Data Traffic into the network and back through the content filter and firewall as needed. Currently the district utilizes Sprint wireless data services as the cellular data provider and is connected with Sprint’s Data Link network solution. Yes, the Managed Internet Service Provider will manage any District VPN’s and currently that is the Data Link solution.
7. Section 3.3:7, SRST normally included local B-1 or PRI in the event of network failure. This question says to replace POTS with a T-1. How will remote survivability be maintained in the event of network failure?
   a. Currently the District has POTS lines connected to a SRST router at each campus. In the event of a network failure, only 2-4 outgoing voice connections are supported from the SRST router. It is the goal of

the district to migrate the 2-4 POTS lines (providing only voice/PSTN access) to an IP connection, so that in the event of network WAN failure, the campus will fail over to the secondary WAN in normal operation mode but with limited WAN bandwidth and not invoke SRST for PSTN access.

8. Describe the intended us of multicast via the Internet. Is this inbound or outbound?

   a. There is no intent or requirement to support multicast via the Internet. The intent is that the Managed Internet Transport Network (MITN) would also serve as a secondary route from/to the data center from the aggregation sites. In the event of a District WAN failure, the district traffic would be routed across the MITN to the destination location both internally or externally.



9. SLA of the Internet performance is not normally offered by any provider. SLA's for Internet normally cover availability. Is section 3.3.2.1 referring to the transport to the public internet, and the ability to reroute to other POPs based on availability?

   a. It is understood that the Managed Internet Service Provider (MISP) cannot guarantee Internet performance; however, the expected service levels of the MITN and the managed hardware should be described.

10. Section 3.3.2.2, Does this assume dedicated connections to multiple Tier 1 providers and not simply public or private peering Points?

    a. See Answer 4 above.

11. Section 3.3.4 wants to allow internet access to external remote users accessing the network via VPN. This is commonly referred to as "hair-pinning" and is normally considered a serious security breach allowing phishing and spoofing using the District's network. Is this the District's intent to allow external users to "hair-pin?"

a. No, it is not the District's intent to allow "hair-pinning" or, with a different connotation/definition, to design "hair-pinning" into the mobility management solution. It is the intent of the district to meet CIPA compliance and District Internet Use Policy requirements that require all District devices to be filtered from unacceptable Internet content. The remote users will be 3G/4G Wireless Devices that use District IP addresses, authenticate hardware to Cellular provider, traverse the provider network via private connection or via VPN over public Internet to the District's Authentication service and then, by policy and access, either utilize District Intranet resources (Staff, Admin) or go through the content filter (all users) to the Internet. The ASA's currently used can support intra-interface traffic (hair-pinning) back to the Internet; however, that is not the requirement and usage.

NOTE:
Please acknowledge receipt of this addendum by signing and dating this page and include a copy with your proposals.

Signature____Date: __________________