Request For Proposal

Prepared for
East Texas Council of Governments (ETCOG)

Request for Proposal ETCOG-100

September 2010

TABLE OF CONTENTS

1. INTRODUCTION 6

1.1 INTENT 7
1.2 INDUSTRY STANDARDS, RECOMMENDATIONS, AND BEST PRACTICES 7
1.3 USE OF THE IP NETWORK FOR NG9-1-1 SERVICES 7
1.4 PROJECT GOALS 8

2. PROPOSAL SUBMISSION INFORMATION 10

2.1 KEY DATES 10
2.2 ETCOG CONTACT INFORMATION 10
2.3 PROPOSAL SUBMISSION PROCESS 10
2.3.1 Respondent Contact Information 10
2.3.2 Proposal Submission Due Date 11
2.3.3 RFP Questions Submission and Answer Process 11
2.3.4 Pre-proposal Meeting 12
2.3.5 Evaluation and Selection Process 12
2.3.6 Respondent Presentations 12
2.4 PROPOSAL SUBMISSION REQUIREMENTS 13
2.4.1 Submission Format and Content 13
2.4.2 Instructions to Respondents 14
2.4.3 Requirements Compliance Responses 15
2.5 EVALUATION PROCESS OVERVIEW 15
2.5.1 General Evaluation Criteria 15
2.6 PRICING 16
2.6.1 Network Pricing Presentation 16
2.6.2 Option Pricing 18

3. GENERAL PROJECT REQUIREMENTS 20

3.1 GENERAL QUALIFICATIONS 20
3.2 EXPERIENCE 20
3.3 PROJECT MANAGEMENT 20
3.4 PROJECT MANAGER 21
3.5 SCOPE OF WORK 21
3.5.1 Progress Reports 21
3.6 KEY STAFF 22

4. GENERAL TERMS AND CONDITIONS 23

4.1 GOVERNING LAW 23
4.2 GOVERNING FORMS 23
4.3 ADDENDA 23
4.4 PIGGYBACK PROVISIONS 23
4.5 HOLD HARMLESS AGREEMENT 23
4.6 WAIVER OF SUBROGATION 23
4.7 HISTORICALLY UNDERUTILIZED BUSINESS (HUB) PARTICIPATION 24
4.8 APPEAL CRITERIA 24
4.9 NO FINANCIAL INTEREST OR OTHER CONFLICT 24

4.10 SEVERABILITY 24
4.11 TAXES 25
4.12 FISCAL FUNDING 25
4.13 PRICING 25
4.14 SILENCE OF SPECIFICATIONS 25
4.15 SUPPLEMENTAL MATERIALS 25
4.16 OPEN RECORDS 26
4.17 INSPECTIONS 26
4.18 TESTING 26
4.19 DISQUALIFICATION OF RESPONDENT 26
4.20 AWARD 26
4.21 ASSIGNMENT 26
4.22 TERM CONTRACTS 27
4.23 PIGGYBACK PROVISIONS 28
4.24 MAINTENANCE 28
4.25 CONTRACT OBLIGATION 28
4.26 TITLE TRANSFER 28
4.27 WARRANTIES 28
4.28 DELIVERY 29
4.29 CONTRACT RENEWALS 29
4.30 INVOICES AND PAYMENTS 29
4.31 TERMINATION 29
4.32 RECYCLED MATERIALS 29
4.33 SCANNED OR RE-TYPED RESPONSE 30
4.34 CONTRACT TERM AND OPTION TO EXTEND 30

5. IP NETWORK 31

5.1 PROJECT GOALS 31
5.2 GENERAL TECHNICAL REQUIREMENTS 31
5.2.1 Open Standards 32
5.2.2 Scalability 32
5.2.3 Architectural Survivability 32
5.2.4 Network Upgrades and Maintenance 33
5.2.5 Bandwidth 33
5.2.6 Network - ETCOG Interface 33
5.2.7 IP addressing 33
5.2.8 IP Routing 34
5.2.9 Quality of Service 34
5.2.10 Network Address Translation (NAT) 35
5.3 AUXILIARY IP NETWORKS 35
5.4 NETWORK MONITORING 36
5.4.1 Network Fault Management 36
5.4.2 Network Performance Management 36
5.4.3 Information Retrieval 37
5.5 NETWORK MANAGEMENT 37
5.5.1 Network Configuration Management 37
5.5.2 Configuration Restoration 37
5.5.3 Root Cause Analysis (RCA) 37

5.5.4 Preventative Maintenance ... *37*
5.5.5 Scheduled Maintenance ... *37*
5.5.6 Security Monitoring and Management ... *37*
5.6 TRANSIENT VOLTAGE SURGE SUPPRESSION (TVSS) ... 38
5.7 SPARES ... 38
5.8 NEW ORIGINAL EQUIPMENT MANUFACTURER (OEM) EQUIPMENT ... 38
5.9 SERVICE LEVEL AGREEMENTS ... 39
5.10 NETWORK AND ACCEPTANCE TESTING PROCESS ... 39

6. EMERGENCY TELEPHONE SYSTEM ... 40

6.1 CURRENT LONGVIEW CPE CONFIGURATION ... 40
6.2 GENERAL TECHNICAL REQUIREMENTS ... 41
6.2.1 System Sizing and Functions ... *41*
6.2.2 Standards Requirements ... *41*
6.2.3 Required NG9-1-1 Features ... *42*
6.2.4 Call Transfer Interoperability over IP ... *42*
6.2.5 System Monitoring and Notification ... *42*
6.3 CPE PRICING ... 43
6.4 IMPLEMENTATION ... 44
6.4.1 Training ... *44*
6.4.2 Dual System Cutover ... *44*
6.4.3 Pre-cutover Acceptance Testing ... *44*
6.4.4 Certification ... *44*
6.4.5 Acceptance Testing ... *44*
6.4.6 Fail-over Strategy ... *44*
6.4.7 Production Test ... *44*
6.4.8 Post-cutover Final Acceptance Testing ... *45*
6.4.9 Post-installation Follow-up ... *45*
6.4.10 PSAP Interface Wiring, Dmarc, Labeling, and Site Records Requirements ... *45*
6.4.11 Drawings/Software ... *45*
6.5 MIGRATION STRATEGY ... 45
6.6 TRANSITION AND DEPLOYMENT ISSUES ... 45

7. CHAMPION EMS ANSWERING POSITIONS ... 47

7.1 SCOPE ... 47
7.2 GENERAL TECHINCAL REQUIREMENTS ... 47
7.2.1 Standards Requirements ... *47*
7.2.2 Required NG9-1-1 Features ... *47*
7.3 CPE PRICING ... 48
7.4 IMPLEMENTATION ... 49
7.4.1 System Installation ... *49*
7.4.2 Pre-commissioning Acceptance Testing ... *49*
7.4.3 Certification ... *49*
7.4.4 Acceptance Testing ... *49*
7.4.5 Fail-over Strategy ... *49*
7.4.6 Production Test ... *50*
7.4.7 Post-cutover Final Acceptance Testing ... *50*
7.4.8 Post-installation Follow-up ... *50*

7.4.9 Site Management *50*
7.4.10 PSAP Interface Wiring, Dmarc, Labeling, and Site Records Requirements *50*
7.4.11 Drawings/Software *50*
7.5 TRANSITION AND DEPLOYMENT ISSUES 50

8. APPENDIX A – ETCOG CONCEPTUAL NETWORK DESIGN 52

9. APPENDIX B – SERVICE LEVEL AGREEMENTS 54

9.1 NETWORK PERFORMANCE 54
9.1.1 Voice Quality and Quality-of-Service *54*
9.1.2 Network Latency *54*
9.1.3 Packet Loss *55*
9.1.4 IP Deviation Variance (IPDV) (Jitter) *55*
9.1.5 QoS *55*
9.1.6 Redundant Recovery Time *55*
9.1.7 Network Availability *55*
9.1.8 Field Response Time and Mean-Time-to-Repair *55*
9.1.9 Service Level Agreement *55*
9.2 NETWORK MONITORING 56
9.2.1 Reporting and NOC Operations *56*
9.3 REMEDIES 56

10. APPENDIX C – GLOSARY 57

11. ATTACHMENT D – CPE FUNCTIONAL REQUIREMENTS 64

1. INTRODUCTION

The East Texas Council of Governments (ETCOG) is a regional voluntary association of counties, cities, and other agencies across fourteen counties. The region covers an area of 10,000 square miles. The January 1, 2009 population estimate for the region is 809,000.

ETCOG is one of twenty-four regional associations in Texas. Created in 1970 in response to the regional Planning Act of 1965, as amended and codified, ETCOG is defined as a political subdivision of the state. In part the law provides that "The counties and municipalities making the agreement may join in the exercise of, or in acting cooperatively in regard to, planning, powers, and duties as provided by law for any or all of the counties and municipalities." (Texas Local Government Code, Title 12, Chapter 391.003e.)

Through this request for proposal (RFP) ETCOG desires to implement a managed and private Internet protocol (IP) network that will be the foundation of a public safety IP infrastructure for the ETCOG service area. This initial deployment of the IP network will interconnect twenty one sites: Eighteen ETCOG PSAPs, the Kilgore Police Department, the Longview Police Department, and the ETCOG office.

Also through this RFP the City of Longview Police Department wishes to procure a next generation capable Emergency Telephone System, to replace the existing Positron Lifeline ANI/ALI controller system at that location. The new Longview PD Emergency Telephone System (ETS) must interconnect with the IP network that is part of this proposal, and must support next generation 9-1-1 (NG9-1-1).

Also through this RFP Champion EMS wishes to procure PSAP answering positions. These positions may be hosted off of an existing PlantCML Vesta Pallas ANI/ALI controller located at Gregg County, and interconnected to Champion EMS via the IP network that is part of this RFP. Alternatively a complete standalone NG9-1-1 capable PSAP solution may be proposed. In the second case the system must be able to accept transfer calls with full ALI information from the existing PlantCML Vesta Pallas sites over the IP network, as well as accept SIP calls from any source

Respondents may submit proposals for the ETCOG IP network only, for the Longview PD ETS only, for the Champion CPE only, or for any combination. Awards for these systems will be considered separately.

The Respondent's submittal to this RFP will be for a complete "turn-key" managed IP network solution and/or for an Emergency Telephone System that includes (but is not limited to): design, project management, implementation, testing, certification, and maintenance.

For the IP network solution, the Respondent's submittal must also include network performance monitoring, logging and reporting, and the use of a Network Operations Center. IP network proposals must also include a network security <u>option</u> that provides network security monitoring and a security operations center. These functions may be integrated with a Network Operations Center or with other network elements, at the Respondent's discretion.

Other options may be proposed at the Respondent's pleasure, however, items or services that are part of the base requirements may not be listed as "optional," and must be included in the base pricing.

Respondents must specify in their proposals a well-defined procedure for ETCOG to place change orders after the network is implemented and accepted.

1.1 INTENT

The purpose of this RFP is to communicate ETCOG's plans to contract for a scalable, standards-based, interoperable, carrier agnostic, and managed IP network solution. It is the intent of ETCOG that this RFP encourage creativity and competition in the service provider community. To this end ETCOG will be holding a period of open questions, a pre-submittal Respondents meeting, and then a second period of open questions, before the proposal due date.

The purpose of the pre-submittal Respondents meeting and the two open question periods is to assure Respondents understanding of ETCOG's requirements and the scale and scope of the solution(s) desired, and to clarify, in writing, any questions concerning this RFP. ETCOG seeks responses of the highest quality and responses targeted to ETCOG's plans. Therefore attendance at the pre-submittal meeting and Respondent's participation in the open question process, while not mandatory, is greatly encouraged.

1.2 INDUSTRY STANDARDS, RECOMMENDATIONS, AND BEST PRACTICES

Adherence to industry-accepted recommendations and best practices provides many advantages, including protection from obsolescence, improved supportability, reduced costs, and improved interoperability. For these reasons, ETCOG places a great deal of importance on standards and best practices.

Respondents are required to be aware of, and present proposals based upon, applicable Internet Engineering Task Force (IETF) request for comments (RFCs), National Emergency Number Association (NENA) recommendations for Emergency Services IP networks (ESInets,), and recommendations of the Federal Communication Commission's (FCC) Communications Security, Reliability, and Interoperability Council (CSRIC – formerly NRIC) applicable to 9-1-1 networks.

The proposed IP network must comply with applicable IETF RFCs such as, but not limited to, Internet protocol, IP routing, Quality-of-Service (QoS), and Network Monitoring (SNMP). The proposed IP network must be capable of supporting Session Initiation Protocol (SIP) and provide high quality transport of Real-time Transport Protocol (RTP) media streams such as G.711. Within bandwidth constraints the proposed network must be voice-over Internet protocol (VoIP) ready.

The proposed ETS must comply with applicable National Fire Protection Association (NFPA) 1221 standards for the installation, maintenance and use of emergency services communications systems.

1.3 USE OF THE IP NETWORK FOR NG9-1-1 SERVICES

It is the intent of ETCOG to migrate to NG9-1-1 services when, in ETCOG's judgment, these services are fully developed, when they can be deployed in a cost effective and sustainable manner, and as these services meet the needs of public safety in the ETCOG region.

This first deployment of the public safety IP network will provide infrastructure which ETCOG needs to accomplish several first steps towards the ultimate goal of implementing NG9-1-1 across the ETCOG region. Although not part of this RFP except as specified, these initial activities include: migration of an existing geographic information services (GIS) application to the new IP network, call transfer among PSAPs using the IP network as transport, and ANI/ALI controller consolidation among the PSAPs using the IP network as transport.

The initial and the recurring cost of the IP network is a significant concern to ETCOG. In an attempt to control those costs, the base IP network requirements as specified herein will be limited, satisfying the needs of the planned initial

uses of the IP network while providing comparable levels of service to existing networks. Later procurements will expand this foundational IP infrastructure to include more sites, to increase bandwidth, and to improve service levels as the uses of the IP network justify these increased costs. Respondents are required to provide information to ETCOG about how their proposed solutions will scale, and the likely costs associated with such future expansion.

ETCOG is not requesting that the proposed IP network infrastructure meet all present or anticipated standards or requirements for an ESInet. However, ETCOG expects that the proposed IP network will become the foundation of a future ETCOG ESInet infrastructure. ETCOG must assure that the proposed network can be reasonably upgraded to meet these future requirements.

It is also anticipated that this IP network will eventually interconnect with several Emergency Communications Districts (ECDs) within the ETCOG region, and will interconnect with other regional and/or state-level public safety IP networks or ESInets in Texas. The design and implementation of the core IP network must support these future connections with reasonable incremental costs.

1.4 PROJECT GOALS

The ETCOG's 18 PSAPs, Kilgore and Longview Police Departments, and the ETCOG administrative office will connect to and be served by the proposed new open-architecture managed IP network.

ETCOG hopes to gain many benefits by eventually transitioning from proprietary and purpose-built legacy 9-1-1 hardware to a network based on commercial off-the-shelf (COTS) components and based on open standards. The benefits that the ETCOG is seeking include:

- increasing the reliability and resiliency of the 9-1-1 delivery network
- providing flexibility to easily integrate new technology
- the ability to more easily extract management data via the network
- equalizing service levels across the ETCOG area
- improving call transfer functionality
- improving communications among the PSAPs, police departments, and ETCOG office
- facilitating a cooperative project initiative involving all stakeholders
- improving public safety for the citizens of and visitors to the region while controlling costs

To realize these project goals the new ETCOG IP network must reduce or eliminate single points of failure in its design, including designing redundant connections to selected network sites. Such proposed redundant faculties should also be as diverse as is economically possible.

ETCOG recognizes that facility limitations in some areas of the region may result in proposals that are not fully diverse, particularly with respect to "last mile" connections to PSAP sites. ETCOG requests Respondents to be as creative as possible in mitigating any lack of diversity for redundant facilities. For example, microwave or cable infrastructure might be used to provide an alternative to terrestrial fiber or copper when no diversity is available in the terrestrial plant. Limitations on diversity, and any mitigations proposed, shall be fully explained in proposals.

ETCOG is planning on utilizing this network to consolidate PSAP telecommunications customer premise equipment, (CPE) as listed in the following table. This is for Respondents information only, as the actual reconfiguration of the CPE equipment is outside the scope of this RFP. However, the Respondent will be required to provide redundant connections to the specified ANI/ALI controller host sites. The CPE at all sites is the PlantCML Vesta Pallas, except Kilgore PD uses a PlantCML Patriot, and Longview PD currently has a Positron Lifeline that itself is a subject of this RFP. The ETCOG office currently does not have 9-1-1 call taking equipment.

Base proposals for the IP network must provide IP connectivity to the specified twenty one sites at the locations listed in the table below, and in accordance with the requirements listed in this RFP.

Site Name	Street (physical location)	City	County	CPE Host Site	Redundancy Required
Anderson County Sheriff's Office	1200 E Lacy	Palestine	Anderson	Yes	Yes
Camp County Sheriff's Office	203 Tapp Street	Pittsburg	Camp		
Canton Police Department	24980 State Highway 64	Canton	Van Zandt		
Carthage Police Department	321 W Panola	Carthage	Panola		
Champion EMS Gregg County	2201 South Mobberly	Longview	Gregg	TBD	Yes
Cherokee County Sheriff's Office	5275 Underwood	Rusk	Cherokee		
ETCOG Office	3800 Stone Rd	Kilgore	Gregg		Yes
Gladewater Police Department	511 S Tyler	Gladewater	Gregg		
Gregg County Sheriff's Office	101 E Methvin, STE 559	Longview	Gregg	Yes	Yes
Jacksonville Police Department	210 W Larissa	Jacksonville	Cherokee		
Kilgore Police Department	909 North Kilgore St.	Kilgore	Gregg		
Longview Police Department	302 W. Cotton Street	Longview	Gregg		Yes
Marion County Sheriff's Office	102 W Austin	Jefferson	Marion		
Mineola Police Department	300 Greenville Highway	Mineola	Wood		
Palestine Police Department	511 N John	Palestine	Anderson		
Panola County Sheriff's Office	314 Wellington Street	Carthage	Panola	Yes	Yes
Rains County Sheriff's Office	313 N Street	Emory	Rains		
Upshur County Sheriff's Office	405 N Titus	Gilmer	Upshur	Yes	Yes
Van Zandt County Sheriff's Office	1220 W Dallas	Canton	Van Zandt	Yes	Yes
White Oak Police Department	103 E Old Hwy 80	White Oak	Gregg		
Wood County Sheriff's Office	402 S Stephens	Quitman	Wood	Yes	Yes

Although not part of the CPE consolidation effort, redundant connections are also required to the Champion EMS, ETCOG office, and to the Longview PD sites.

Respondents shall define and design a network architecture and topology that best meets the requirements of this RFP and its intended future expansion. The network design will be evaluated to determine how well it supports and fulfills both the immediate and long-term goals of ETCOG.

The awarded vendor will plan, design, install, test, certify, and operate the ETCOG IP network.

2. PROPOSAL SUBMISSION INFORMATION

The following key information is offered to assist potential respondents information regarding the critical dates and processes associated with successfully submitting their proposal(s).

2.1 KEY DATES

The urgency of this project is necessitated by ETCOG's annual fiscal budgeting process, which will require an aggressive schedule of events for the RFP process. The currently planned dates for the procurement process are:

RFP release date	September 10th, 2010
Questions due (Round #1)	September 21th, 2010
Pre-proposal meeting (Call bridge will be made available)	September 28th 2010
Questions due (Round #2)	October 5th 2010
Proposals due	October 15th 2010, 5PM CDT
Potential presentation date(s)	October 26th – 28th 2010
Possible initiate contract negotiations	November 8th - 10th 2010

2.2 ETCOG CONTACT INFORMATION

All contact with ETCOG with respect to the IP network procurement, and any questions concerning this RFP or submittal of the proposal should be directed to:

Mailing and Physical Address

Attention: Ms. Carolyn Flores
Director of 9-1-1 Emergency Services
East Texas Council of Governments
3800 Stone Road
Kilgore, TX 75662
903 984-8641 ext 234
Carolyn.Flores@ETCOG.org

2.3 PROPOSAL SUBMISSION PROCESS

2.3.1 Respondent Contact Information

Interested potential Respondents will provide the name (designee), address, telephone number, facsimile number, and email address of the person who should be contacted concerning questions regarding the RFP response(s), via letter or email to Carolyn Flores, by the pre-proposal meeting date, as listed above. This action does not constitute a commitment on the part of a Respondent to submit a proposal. This contact information will be used to provide

interested parties a direct distribution of updates, changes, and informational postings regarding this procurement. ETCOG will distribute formal RFP addenda, RFP questions and responses, and other information to the aforementioned Respondent designated contact, as well as post such information on the www.etcog.org site.

2.3.2 Proposal Submission Due Date

All proposals must be sealed and delivered to the ETCOG office at the time and date outlined in the table above in Section 2.1.

ETCOG requires ten bound hard copies of each proposal, one soft copy of each proposal, and one soft copy of a Microsoft Excel spreadsheet containing pricing, equipment lists, and any other data. The preferred method of soft copy delivery is by USB Flash drive or CD/DVD-ROM in .pdf, Microsoft Word, and/or Microsoft Excel format(s).

Respondents must assume full responsibility for timely delivery and receipt of sealed proposals at the ETCOG office at the address provided above. The receipt of the proposal package must be logged-in by an ETCOG staff member. Proposals which for any reason are not so delivered will not be considered. Late proposals will be returned to the Respondent unopened. The mere fact that a proposal was mailed or sent to ETCOG will not be considered as complying with this requirement and will not be accepted if received after the date and hour set as the submission deadline for any reason, including being delayed in the internal mail system of ETCOG. Unsealed proposals, which are received at the above address by any means, will not be considered.

Only printed hard copy proposals with accompanying soft copy are accepted. Proposals by telegram, telephone, email, oral, or facsimile reproduction and transmission will not be considered. Late submissions will not be accepted for any reason.

Note: ETCOG offices are closed from Noon to 1:00 p.m. each day. Respondents must take this into account when planning hand delivery of proposals or delivery by private carriers.

2.3.3 RFP Questions Submission and Answer Process

ETCOG intends to conduct two written rounds of questions and answers; one prior to and one quickly following the pre-proposal conference according to the schedule outlined in Section 2.1.

All Respondent questions with respect to this RFP shall be received in soft copy format only, according to the deadlines as outlined above, to Ms Carolyn Flores, using either a Microsoft Word file attached to an email, or in the text of the email itself. If email 'delivery' or 'read' receipts are requested, they will be acknowledged and returned.

All official ETCOG responses to Respondent questions will be supplied in a soft copy format and distributed to the designee's email address of all participating Respondents, as designated in Section 2.3.1. This RFP and all official addenda, and questions and answers will also be posted on the ETCOG web site at www.etcog.org. ETCOG will not be responsible for any designee's failure to receive any email for whatever reason.

Only these official written responses to questions are considered the official responses of ETCOG in this procurement. All other responses to questions posed, whether written or oral, should be considered unofficial and will not necessarily be incorporated into the official documentation of the project. ETCOG will assume no responsibility for any unofficial answers, regardless of who provided an unofficial answer or under what circumstances the answer may have been offered.

There will be no official responses supplied to questions outside of the described soft copy format or after the question deadlines as outlined in Section 2.1.

2.3.4 Pre-proposal Meeting

Respondents interested in submitting a proposal in response to this RFP should attend the Respondent's conference at the time indicated above in Section 2.1.

The meeting will be held at 10 AM Sept 28th in the ETCOG office, 3800 Stone Rd, Kilgore, TX. The meeting is expected to last up to two hours.

The meeting attendance is limited to four persons per potential respondent or proposal team.

2.3.5 Evaluation and Selection Process

Qualified proposals that are received prior to the submission deadline will be logged-in immediately. Qualified proposals will be distributed to the ETCOG Selection Committee after the submission deadline. Proposals will then be unsealed and will be evaluated by the Selection Committee.

The ETCOG Selection Committee will complete initial evaluations. At any time during the evaluation process, ETCOG reserves the right, where it may serve ETCOG's best interest, to request additional information or clarifications from Respondents.

ETCOG reserves the right to waive any or all irregularities, formalities, or other technicalities. ETCOG will be the sole and independent judge of the quality and the suitability of any proposal, product, or service offered. ETCOG may accept or reject any proposal in its entirety, or may reject any part of any proposal, without affecting the remainder of that proposal. ETCOG reserves the right to self-provision.

ETCOG, at its sole discretion, reserves the right to negotiate with one, several, or none of the respondents submitting proposals against this RFP.

If more than one Respondent is selected for contract negotiations by ETCOG, they will be ranked in order of preference by the Selection Committee and final contract negotiations will begin with the top ranked vendor. Should negotiations with the highest ranked vendor fail to yield a contract, or if the vendor is unable to execute said contract, negotiations may then commence with the second highest ranked vendor, etc.

It is understood that ETCOG, through its management and/or its members, may use all means at their collective disposal to evaluate the proposals received based on the stated criteria. The final decision as to the suitability of the products and/or services offered will rest solely with ETCOG or its designee(s). ETCOG reserves the right to select the vendor of choice regardless of price.

It is anticipated that the highest ranking Respondent(s) will be notified of their initial selection on or about November 6th, 2010, with contract negotiation discussions and execution initiating soon thereafter. The successful Respondent(s) will be notified by a "Notice of Intent to Negotiate" issued by ETCOG's management.

By submission of a response, Respondent indicates acceptance of the evaluation technique, and recognizes and accepts that ETCOG and its representatives may at its sole discretion make subjective judgments during the evaluation process.

2.3.6 Respondent Presentations

At the discretion of ETCOG, Respondents may be invited to make presentations/demonstrations in order to further clarify the invited Respondent's proposed solution(s). If invited, ETCOG will give as much notice as possible to the Respondent to prepare for the presentation. An invitation, if any, does not constitute acceptance of that proposal or rejection of any other proposal(s).

If a presentation is requested it may include detailed drawings, whiteboard drawings, demonstrations of required and recommended functionality, and other methodologies to help the evaluation committee understand the functionality and value of the proposed solution. ETCOG may provide guidance on aspects of the proposal that require further clarification with the invitation.

Respondents are highly encouraged to offer optional solutions that are above and beyond the requirements of the basic ETCOG public safety IP network that is the subject of this RFP. It is expected that a presentation, if invited, will provide the Respondent/team an opportunity to expound upon the attributes and capabilities of their proposed solution(s), including any optional features or services proposed.

2.4 PROPOSAL SUBMISSION REQUIREMENTS

2.4.1 Submission Format and Content

This RFP has been provided as an electronic file. This file, together with the official soft copy responses to questions as discussed in 2.3.3 above, and together with any addenda to the RFP, if any, collectively represents the entire RFP.

These files will be posted on the www.etcog.org web site. It is the Respondent's responsibility to review the web site and insure that the Respondent has obtained all official documents related to the RFP.

It is the Respondent's responsibility to be thoroughly familiar with all requirements and specifications. It is the Respondent's responsibility to assure that each proposal addresses each element of the RFP package, and includes each item described below before it is submitted to ETCOG.

2.4.1.1 Transmittal Letter

Each response must include a 'Transmittal Letter' indicating the Prime firm's company name, address, and the signature (IN INK) of an officer of the company who has signatory authority for a proposal of the total value, including all options, as indicated on the included pricing sheets.

2.4.1.2 Comprehensive Proposal Narrative Response

All Respondents are encouraged to submit concise and clear proposals consistent with the format outlined herein. Proposals that do not comply with this format, are of excessive length, or contain a preponderance of "boilerplate" text, are strongly discouraged. ETCOG encourages Respondents to provide thorough responses to each of the RFP sections in narrative form. Tailored information which describes the Respondent's approach and deliverables that demonstrate the Respondent's knowledge and competence are encouraged.

To the greatest degree possible, this narrative response should be provided in the same order, same outline sequencing, and with the same section numbers, as is provided in the RFP. This will aid ETCOG in reviewing, understanding, and evaluating the content of each Respondent's response

Of particular interest to ETCOG is a thorough presentation by the 'Prime' vendor regarding the proposed plan for project management, subcontractor management (if applicable,) integrated and coordinated project scheduling, phasing and staging of the project across multiple fiscal years, and other information that outlines how the project can be completed within the available project schedule, resources, and funding.

Vendors should take early note of the following items. It is important that questions regarding this information be identified and clarified as early as possible in the process:

2.4.1.3 Bandwidth Requirements

The minimum bandwidth for any link in the IP network will be a DS1 or DS1 equivalent of 1.5 Megabits per second.

Non-Redundant sites must have a Committed Information Rate (CIR) from the site to the core IP network of at least 0.5 megabits per second.

Redundant sites must have an aggregate CIR from the site to the core IP network of at least 1.0 megabits / second, except Gregg County Sheriff's Office and Panola County Sheriff's Office must have aggregate CIR from each site to the core IP network of at least 1.5 megabits / second.

The CIR between any two POIs that are part of the core network must be greater than the smaller sum of the CIRs of all the sites that connect to the POI. In addition, if the proposed network contains more than two POIs, the total aggregate CIR from any POI to the core network must not be less than the sum of the CIRs of all the sites connecting to that POI. Both of these conditions must hold concurrently.

Respondents are requested to consider the implications of additional future interconnections to any POI, and allow for an incremental growth path of at least 50% greater than the initial bandwidth requirements.

2.4.1.4 Appendix A – ETCOG Conceptual Network Design Diagram

This diagram is provided as an overview to illustrate logical network architecture only. It is not a specified physical or topological network design. ETCOG encourages Respondents to submit a proposed network design that is uniquely their own, and which delivers the identified performance and functionality most efficiently, cost effectively, and reliably for ETCOG.

2.4.1.5 Appendix B – Service Level Agreements

This document provides requirements for IP network performance, and for providing network management reports and data.

2.4.1.6 Appendix C – Glossary

2.4.1.7 Appendix D – PSAP CPE Requirements

2.4.2 Instructions to Respondents

The requirements are drawn from the customer's perspective, and therefore do not specify each and every element necessary for the Respondent to deliver the specified results. The Respondents are the experts and are expected to design, recommend, and implement the most effective and efficient solutions at the lowest price. Respondents are encouraged to provide information regarding improvements or alternatives to requirements in their response.

Respondents must address each requirement. Where requested, the Respondent shall supply concise, plain language written descriptions of how the requirement will be satisfied. Responses shall be accompanied with diagrams and other graphical aids as required or as the Respondent finds useful. Merely repeating the requirements may be considered non-responsive and may disqualify the Respondent.

Explanations should be written for a target audience that has 9-1-1 experience but that is generally not expert in IP networks. However, responses to technical requirements may assume a level of technical expertise consistent with the requirements. Excessive use of acronyms or highly technical terms should be avoided. Attempts to hide behind jargon or the failure to make clear to a reasonably knowledgeable reader how a requirement is satisfied will be viewed as non-responsive. Explanations that market a solution rather than explain how the requirement will be satisfied will negatively impact the evaluation of the response. Drawings or diagrams must not be cluttered with irrelevant information or unexplained or obscure objects.

No response may direct the reader to refer to a response elsewhere in the document. Wherever a requirement is repeated, the entire applicable response shall also be repeated. Where a requirement requests that other materials

be provided (e.g., a users' manual), the response shall affirm that the material has been provided with the response, and the submitted material shall be marked with the specified attachment number.

2.4.3 Requirements Compliance Responses

Required features are represented by the use of the words must, will, requirement, or required. Respondents must respond to requirements in the form of either:

COMPLY, which indicates that the feature/capability is part of the offering as proposed *and* the feature/capability **is included** in the base pricing of the proposal.

NOT COMPLY, which indicates that the proposed solution does not meet the stated requirement *or* that the feature/capability **is not included** in the base price.

EXCEPTION, indicates that the proposed solution does not meet this requirement as stated, but there is additional information that the Respondent would like to provide. Respondent must indicate with requirement if feature is included or not included in the base price.

Proposals must include a detailed response immediately following each requirement, describing how the proposed solution meets the particular feature/functionality/requirement, or describing restrictions, optional pricing, or alternative compliance. These responses are especially important in the cases of "EXCEPTION" or "NOT COMPLY."

If a Respondent provides supportive collateral material in response to a requirement, those materials must be limited to three pages per requirement and must be identified by the RFP requirement number.

If a Respondent takes EXCEPTION to a particular item, they must provide an alternative proposal that demonstrates how they intend to meet the requirement.

If a Respondent's proposal does not fully meet any requirement, there must be a section in the response labeled Exceptions to Requirements. In this section, every requirement that the proposal does not fully meet must be revealed and a proposed solution must be offered.

A provision for an Exception to Requirements section is not to be construed as ETCOG's willingness to accept proposals that do not meet all requirements. But it is recognized that a potential Respondent may be able to provide a solution that meets or exceeds the desired functionality in a manner that has not been considered by ETCOG in the RFP. ETCOG is willing to consider such alternatives. However, the Respondent must also recognize that proposing such an alternative solution increases the risk that the proposal may be evaluated negatively.

Some features may be listed as desirable. These features are desirable but are not required. Desirable features are represented by the words may, should, desired, or desirable

Requirements as listed in the RFP sections are not all-inclusive, but are meant to provide a list of the general requirements for the ETCOG managed IP-enabled public safety network. Vendors must understand the overall project goals and intentions of ETCOG, and insure their proposal(s) satisfy the goals and intentions.

2.5 EVALUATION PROCESS OVERVIEW

2.5.1 General Evaluation Criteria

The evaluation team will review all documentation and other information received. The evaluation team will evaluate the proposals and will take particular interest in how the responses address these areas:

- quality of the network design
- alignment with ETCOG short and long-term goals and RFP requirements
- cost and value of the proposed solution
- the vendor project management, planning, and scheduling aspects of the proposal
- general criteria, such as vendor references, credentials, and experience

The RFP responses with the exception of the Longview ETS will be scored based on the following weighted criteria

Network design and technical compliance	25 percent
Respondent's service and maintenance experience and strategy	25 percent
Network per site costs for equipment, installation	25 percent
Project management planning and schedule	20 percent
General criteria	5 percent

The RFP responses for the Longview ETS will be scored based on the following weighted criteria

ETS design and technical compliance	30 percent
Respondent's qualifications and experience	15percent
Service and maintenance plan	25 percent
Proposed cost	20 percent
General criteria	10 percent

2.6 PRICING

2.6.1 Network Pricing Presentation

For each and every cost specifically called out, Respondents must list the non-recurring cost and the monthly recurring cost.

Costs must be listed separately for:

- network core elements common to all sites
- monitoring costs associated with the network core
- network elements required to connect each site, listed per site
- monitoring costs associated with each site, listed per site
- any network management costs separate from the costs listed previously

Total of above categories, that is, all network core, site, monitoring, and management costs, herein referred to as the base price.

The costs listed above the Total should be exclusive of each other. Respondents may provide further detail on any of the categories at the Respondents pleasure, but totals for each category must be displayed.

The base price must include all items required by this RFP, including IP network redundancy at the specified nine sites.

The selected Respondent will be held to implementing the IP network in compliance with the requirements of this RFP for the base price during contract negotiations.

Costs must also be listed separately for:

- the network security option, split out in the four categories: management, monitoring, core, and per site as above
- for each non-redundant site, the cost of implementing a redundant connection to the core network
- any other options proposed by the Respondent

These optional items must not be included in the base price.

The pricing presentation is explained in further detail below.

For each cost a description pointing to an equipment list and a list of services, or other narrative, that clearly defines the materials and services included with that cost, must be provided.

The cost of centralized or core network equipment or services that are not associated with an ETCOG location will be displayed separately from the per-site pricing. Centralized equipment will include the cost of shelves or empty card slots in which site-connecting ports may be installed.

Each ETCOG location (PSAP site, police station, or ETCOG office) must have pricing that represents the total monitoring cost associated with that site, and a separate cost for all the network elements required to establish network connectivity at that site, from the shelf or empty card slot in the core to the network demark at the site. If several sites have the same per-site cost, then that cost may be displayed only once, provided the criteria for a site to qualify for that price are clearly stated, and a list of the sites eligible for that price is provided.

For each site that is not provided with redundant network connections, the incremental non-recurring and recurring costs must be displayed for all items and services required to add a redundant connection at that site. These numbers are not included in the total base price.

A narrative on how the network core costs and the per-site costs scale with the addition or removal of network sites, including connections to other ECDs, regional, or state-level IP networks, must be included.

The total monthly recurring and the total non-recurring cost for the entire base project must be provided. These totals will represent the sum of all of the base per-site recurring and non-recurring costs, plus the sum of all the base network core recurring and non-recurring costs, and will include the cost of redundancy at the specified sites.

2.6.1.1 Maintenance Pricing

It is required that all equipment be covered by a vendor 24/7/365 warranty for all parts, labor, and travel without restriction, for one year, as part of the initial installation. The one year period will begin when the network has successfully completed all tests and has been accepted by ETCOG in accordance with the negotiated contract. The cost of this warranty period must be bundled with the non-recurring cost of the network core and the non-recurring cost per-site, and be listed as one of the services included in these cost items. Alternatively, the one year warranty period costs may be itemized, but in any event this cost must be included in the total non-recurring cost of the network.

Respondents must quote pricing for a 24/7/365 annual maintenance contract with service levels similar to the warranty period for succeeding years. Any product or service NOT covered, or any restrictions or limitations on the maintenance service, must be clearly spelled out. Maintenance pricing must be listed for the network core and for each location. Maintenance contracts for succeeding years should not be included in any recurring or non-recurring totals.

Other available maintenance options should be listed, including any options that permit ETCOG to play a role in maintenance.

All terms and conditions of the warranty and succeeding maintenance contracts must be listed in the response.

2.6.1.2 Managed Services

Respondents responding to this RFP must detail the cost of their managed services, as well as describe the added value brought by their managed service offering

Respondents are to be very specific as to exactly what managed services they are offering, to what systems/devices/functions, to disclose any limitations or restrictions, and explain any options, if offered. Respondents are encouraged to provide itemized pricing for their managed services. At the very least, this cost must be listed as a separate line item for the recurring network core costs and for the recurring costs for each network site. Managed services costs must be included in the base price of the network.

2.6.1.3 Project Management

Respondents are required to provide project management for the implementation of the ETCOG IP network. The cost of project management must be bundled with the non-recurring cost of the network core and the non-recurring cost per-site, and listed as one of the services included in these cost items. Alternatively, project management costs may be itemized, but in any event this cost must be included in the total non-recurring cost of the network.

2.6.2 Option Pricing

2.6.2.1 Security Monitoring and Services

Respondents are required to submit an option for Network Security Monitoring functions and service and for a Security Operations Center (SOC). The SOC may be integrated with a Network Operations Center or other network elements at the Respondent's pleasure.

Respondents offering these services should be familiar with relevant industry best practices, and with NENA document 75-001, "NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)." The NENA document can be obtained at http://www.nena.org/standard/NG9-1-1_Security.

Respondents should be very specific as to exactly what security services they are offering, and what devices, tools, and/or monitoring they provide as part of this service.

Pricing for this option should be listed separately for the network core (if applicable) and for each site at which monitoring occurs. These costs should be divided into recurring and non-recurring costs. Totals for a complete security implementation must be included, including any facilities required to interconnect the ETCOG public safety IP network and the SOC, if applicable. The costs associated with Security Monitoring and services should not be bundled with the network base price as described in 2.6.1 above.

ETCOG may elect to exercise this option at ETCOG's sole discretion. Alternatively, ETCOG may choose to obtain these services from another vendor at ETCOG's sole discretion.

2.6.2.2 Use of Auxiliary IP Network for Transport

Respondents are encouraged to submit an option that will permit the use of an "auxiliary" IP network to provide point-to-point IP connectivity between ETCOG-specified network sites, by means of secure IP tunneling through the auxiliary IP network. The technical details of this option are specified in Section 5 of this RFP.

Such a connection may be used to provide an additional layer of redundancy, diversity, and/or bandwidth to the ETCOG public safety IP network, but only as a secondary or tertiary connection, and never as a component of the primary ETCOG public safety IP network, and never as the first redundant connection to a site where redundancy is required.

ETCOG will consider this option a “value-added” feature of the proposal.

This feature may be ordered by ETCOG on a case-by-case basis, at ETCOG’s sole discretion.

Budgetary pricing for this option should be listed as the cost per IP tunnel, and should include required ports, configuration, and monitoring. The cost should be separated into recurring and non-recurring charges, as appropriate. Actual use of this option in a particular circumstance may involve a negotiation between the vendor and ETCOG.

The balance of this page is intentionally left blank.

3. GENERAL PROJECT REQUIREMENTS

3.1 GENERAL QUALIFICATIONS

Respondents must demonstrate its respective organization's competence, qualifications, and ability to perform the services requested by this RFP. This will be measured by several factors, including but not limited to the number of years that the Respondent has provided the services required by the RFP. Respondents should include information on structure, responsibilities, history of partnerships, and alliances collaborating on similar projects. Respondents shall provide a statement from a financial officer of the company who can assure sufficient budget and processes are available to fulfill RFP obligations.

As necessary and applicable, to provide the services and/or equipment in the proposals, the Respondent shall obtain all required certifications, permits, etc. to provide the services and/or equipment to ETCOG in Texas, and shall include certificate numbers assigned as applicable.

3.2 EXPERIENCE

Respondent shall provide the following:

A listing of three references, wherein Respondent provides services similar to those required by the RFP; a brief description of the service; the dates it has provided the service in that jurisdiction; the name, telephone number, and email address for the current customer manager or project director wherein Respondent provides the service.

For the most recent reference, Respondent must supply a brief description of the total project cost and a brief summary of the project outcome. ETCOG is specifically interested if the project closed on budget or with a budget overrun or under-run, and whether the project completed ahead, on, or behind schedule.

ETCOG reserves the right to verify all information provided via direct contact with the reference, and Respondent agrees to provide any release necessary for ETCOG to check the information provided by Respondent. Misstatements are grounds for disqualification of the proposal.

3.3 PROJECT MANAGEMENT

The Respondent must provide a project management plan. Respondents must describe how they will provide project management expertise for this project. The project management section must address the following items:

- Respondent - ETCOG communications plan
- proposed/tentative project schedule, to include milestones, major tasks
- work breakdown structure (WBS)
- network site installation procedures
- testing procedures
- acceptance criteria and procedures

3.4 PROJECT MANAGER

Respondent must identify one individual as the project manager with overall responsibility for the Respondent and subcontractor activities, and empowered to speak for the Respondent. The project manager will provide the single point-of-contact for the management and coordination of all aspects of the awarded Respondent's work.

The name and resume of the Respondent's project manager and project manager's work address must be submitted with the proposal.

The Respondent's project manager must have previously worked on similar projects of this magnitude. Respondents must provide an estimate of how much time the project manager will spend at ETCOG to accomplish the successful installation, testing, acceptance, and ongoing support of the requested services.

It is preferred that the Respondent's project manager be a Project Manager Professional (PMP) certified through Project Management Institute (PMI) or be certified by an organization of equal standing.

3.5 SCOPE OF WORK

This RFP and the vendor's proposal should become the basis of the scope of work (SOW) to assure that all requirements are met. As part of contract award, the SOW must be formally submitted by the awarded Respondent to ETCOG and must include the requirements stated in all sections of this document. ETCOG reserves the right to review and reject the SOW if it does not meet with their satisfaction. ETCOG must approve the SOW before execution of the final contract. The awarded Respondent's RFP response will also become a part of the services contract between the awarded Respondent and ETCOG.

3.5.1 Progress Reports

The awarded Respondent must email progress reports to ETCOG monthly, or as requested by ETCOG. At a minimum, each progress report must contain:

- a clear and complete account of the work performed in the reporting period
- an outline of the work to be performed during the next reporting period
- a bar chart or visual display showing the work accomplished by task versus the planned schedule of work specified by the contract and/or the cost schedule
- a discussion of any problems encountered or anticipated that might affect the completion of the contract within the time and fiscal constraints set forth in the contract, together with recommended solutions to such problems; or a comment that no problems were encountered
- a chart showing incremental costs for the reporting period for all services compared to the proposed timeline and the cost schedule or as required by ETCOG
- any other pertinent information, i.e., analysis data

ETCOG may require weekly meetings to discuss items mentioned above. The awarded Respondent is responsible for any and all communication requirements to host the aforementioned meetings, such as, but not limited to, conference bridges and on site meetings.

3.6 KEY STAFF

Respondents must identify in their proposals each key member of its staff who will participate in the project and the nature and scope of each person's responsibilities and duties.

Respondent must submit detailed resumes for all key personnel. ETCOG will not interview the personnel. Resumes, therefore, must give enough information to provide a clear understanding of the individuals' qualifications; inexperienced personnel are not acceptable.

Respondent must demonstrate how its proposed staffing plan will be sufficient to complete the services required in a timely fashion.

The key personnel to work on this engagement, as identified in the proposals, are an important part to the services to be provided. No Respondent-initiated personnel substitutions following contract award will be made without the prior written consent of ETCOG, which shall not be unreasonably withheld. All requested substitutes must be submitted to ETCOG, together with resumes, for ETCOG approval. ETCOG must approve the replacement individual(s).

The balance of this page is intentionally left blank.

4. GENERAL TERMS AND CONDITIONS

4.1 GOVERNING LAW

Respondents shall comply with all applicable federal, state, and local laws and regulations. Respondent is further advised that these requirements shall be fully governed by the laws of the state of Texas and that ETCOG may request and rely on advice, decisions, and opinions of the Attorney General of Texas and on its Attorney concerning any portion of these requirements.

4.2 GOVERNING FORMS

In the event of any conflict between the terms and provisions of these requirements and the specifications, the specifications shall govern. In the event of any conflict or interpretation of any part of this overall document, ETCOG's interpretation shall govern.

4.3 ADDENDA

When specifications are revised, ETCOG will issue an addendum addressing the nature of the change. The addendum will be distributed as soft copy via email to the vendor's designee, as defined in 2.3.1. Addenda will also be posted to the www.etcog.org web site. It is the Respondent's responsibility to insure that copies of all current addenda have been obtained. Respondents must sign the addendum and include such addendum in the returned proposal package

4.4 PIGGYBACK PROVISIONS

The city of Longview (or any other entity besides ETCOG) may enter a contract directly with a vendor selected as a result of this RFP requiring that vendor to perform services and provide equipment pursuant to the RFP. Longview (or any other entity besides ETCOG) will have the same rights and remedies as ETCOG does under this contract. Longview (or any other entity besides ETCOG) will be obligated to pay only for the services and/or equipment they select and are not responsible for paying for services and/or equipment selected by ETCOG or for paying for everything under the contract.

4.5 HOLD HARMLESS AGREEMENT

Contractor, the successful Respondent, shall indemnify and hold ETCOG harmless from all claims for personal injury, death, and/or property damage resulting directly or indirectly from Contractor's actions. Contractor shall procure and maintain, with respect to the subject matter of this proposal, appropriate insurance coverage including, as a minimum, public liability and property damage with adequate limits to cover Contractor's liability as may arise directly or indirectly from work performed under terms of this proposal. Certification of such coverage must be provided to ETCOG upon request.

4.6 WAIVER OF SUBROGATION

Respondent and Respondent's insurance carrier waive any and all rights whatsoever with regard to subrogation against ETCOG as an indirect party to any suit arising out of personal or property damages resulting from Contractor's performance under this agreement.

4.7 HISTORICALLY UNDERUTILIZED BUSINESS (HUB) PARTICIPATION

Contracting opportunities for historically underutilized (disadvantaged) business (HUBs) as defined in Texas Government Code 481.101(1) shall be considered in the procurement process. To satisfy Texas' statutory requirements [Government Code, Chapter 2161, Subchapter D], ETCOG requires all Respondents to supply information in any proposal response listing: (1) the total number of subcontracts and (2) the total number of HUB contracts applicable to the services offered in the response. For purposes of information availability, Respondents are encouraged to include subcontracts with HUBs that provide delivery of a service

A HUB organization will be chosen in the case of a tie.

4.8 APPEAL CRITERIA

Proposals not selected for funding may be appealed only with respect to any fault or violation of law or regulation regarding the review process. Appeals must be filed within ten (10) calendar days of final action with the Director of Workforce Development Programs, shall be in writing addressed to the Director of Workforce Programs and shall indicate the action appealed, the violation which forms the basis for the appeal, and shall be signed by the appellant organization's authorized representative. Fax and e-mail transmittals will not be accepted. The filing of the appeal within the time frame is a condition precedent. There is no relief accorded appellants for not filing within the published deadlines. Hearings shall be conducted in accordance with existing Workforce Development Board and ETCOG procedures. The process for making an appeal is outlined in the Policies and Procedures for Selecting Service Providers for the East Texas Workforce Development Area, which is available upon request.

4.9 NO FINANCIAL INTEREST OR OTHER CONFLICT

Respondents should not contact Board members or elected officials charged with oversight of these programs during the review process to avoid conflicts or the appearance of conflicts or undue influence over the process.

No ETCOG officer, employee, Board of Directors member, ETCOG board or commission, nor family member of any such person, has a financial interest, direct or indirect, in the RespondentRespondentor in any contract the RespondentRespondent might enter into with ETCOG.

No economic or employment opportunity, gift, loan, gratuity, special discount, trip, favor, or service has been, or will be, offered or given to any officer, employee, Board of Directors member, or ETCOG board or commission, nor to any family member of any such person.

By submitting a response to this solicitation, the RespondentRespondentrepresents that it is not in arrears in the payment of any obligations due and owing the State of Texas, including the payment of taxes and employee benefits, and that it will not become so in arrears during the term of the contract if selected for contract award.

4.10 SEVERABILITY

If any section, subsection, paragraph, sentence, clause, phrase, or word of these requirements or the specifications shall be held invalid, such holding shall not affect the remaining portions of these requirements and the specifications, and it is hereby declared that such remaining portions would have been included in these requirements and the specifications as though the invalid portion had been omitted.

4.11 TAXES

ETCOG is exempt from all federal excise, state, and local taxes unless otherwise stated in this document. ETCOG claims exemption from all sales and/or use taxes under Texas Tax Code §151.309, as amended. Texas Limited Sales Tax Exemption Certificates will be furnished upon written request to ETCOG.

4.12 FISCAL FUNDING

A multi-year lease or lease/purchase arrangement (if requested by the specifications), or any contract continuing as a result of an extension option, must include fiscal funding out. If, for any reason, funds are not appropriated to continue the lease or contract, said lease or contract shall become null and void on the last day of the current budgeted funds. After expiration of the lease, leased equipment shall be removed by the Contractor from the using department without penalty of any kind or form to ETCOG. All charges and physical activity related to delivery, installation, removal, and redelivery shall be the responsibility of the Respondent.

4.13 PRICING

Prices for all goods and/or services shall be negotiated to a firm amount for the duration of this contract or as agreed to in terms of time frame. All prices must be printed electronically or written in ink. Where unit pricing and extended pricing differ, unit pricing prevails.

This request for proposals does not commit or obligate ETCOG or ETCOG partners to pay for any costs incurred in the preparation of a response or in advance of the execution of a subcontract. The contract and accompanying budget must be fully executed prior to the program start date. No costs incurred prior to contract execution will be reimbursed.

4.14 SILENCE OF SPECIFICATIONS

The apparent silence of specifications as to any detail, or the apparent omission from the specifications of a detailed description concerning any point, shall be regarded as meaning that only the best commercial practice is to prevail and that only material and workmanship of the finest quality are to be used. All interpretations of specifications shall be made on the basis of this statement. The items furnished under this contract shall be new, unused, of the latest product in production to commercial trade, and shall be of the highest quality as to materials used and workmanship. Manufacturer furnishing these items shall be experienced in design and construction of such items and shall be an established supplier of the item proposed.

4.15 SUPPLEMENTAL MATERIALS

Respondents are responsible for including all pertinent product data in the returned proposal package. Literature, brochures, data sheets, specification information, completed forms requested as part of the proposal package, and any other facts which may affect the evaluation and subsequent contract award should be included. Materials such as legal documents and contractual agreements, which the Respondent wishes to include as a condition of the proposal, must also be in the returned proposal package. Failure to include all necessary and proper supplemental materials may be cause to reject the entire proposal.

4.16 OPEN RECORDS

All proposals that have been submitted shall be available and open for public inspection after the contract is awarded, except for trade secrets or confidential information contained in the proposals and identified as such. Any public request for clearly labeled trade secret or confidential information shall be handled in accordance with the law and procedures in the Texas Public Information Act.

4.17 INSPECTIONS

ETCOG reserves the right to inspect any item(s) or service location for compliance with specifications and the requirements and needs of the using department. If a Respondent cannot furnish a sample of a proposed item, where applicable, for review, or fails to satisfactorily show an ability to perform, ETCOG can reject the offer as inadequate.

4.18 TESTING

ETCOG reserves the right to test equipment, supplies, material and goods proposed for quality, compliance with specifications, and ability to meet the needs of the user. Demonstration units must be available for review. Should the goods or services fail to meet requirements and/or be unavailable for evaluation, the offer is subject to rejection.

4.19 DISQUALIFICATION OF RESPONDENT

Upon signing the proposal document, a Respondent offering to sell supplies, materials, services, or equipment to ETCOG certifies that the Respondent has not violated the antitrust laws of this state codified in §15.01, *et seq*., Business & Commerce Code, or the federal antitrust laws, and has not communicated, directly or indirectly, the offer made to any competitor or any other person engaged in such line of business. Any or all proposals may be rejected if ETCOG believes that collusion exists among the Respondents. Proposals in which the prices are obviously unbalanced may be rejected. If multiple proposals are submitted by a Respondent and after the proposals are opened, one of the proposals is withdrawn, the result will be that all of the proposals submitted by that Respondent will be withdrawn; however, nothing herein prohibits a Respondent from submitting multiple offers for different products or services.

4.20 AWARD

ETCOG reserves the right to award this contract on the basis of the BEST EVALUATED PROPOSAL, regardless of price, and in accordance with the laws of the state of Texas, to waive any formality or irregularity, to make awards to more than one Respondent, to reject any or all proposals.

4.21 ASSIGNMENT

The successful Respondent may not assign, sell, or otherwise transfer this contract without written permission of ETCOG.

4.22 TERM CONTRACTS

If the contract is intended to cover a specific time period, the term will be given in the specifications under SCOPE.

4.23 PIGGYBACK PROVISIONS

If the city (or any other entity besides ETCOG) is going to enter a contract directly with the vendor selected as a result of this RFP for that vendor to perform services and provide equipment pursuant to the RFP, then the RFP should clearly state that such piggybacking may, or will occur and should clarify that the entities that piggyback off the contract will have the same rights and remedies as ETCOG does under the contract. Depending on the intended arrangement, the RFP should also clarify that the city or other entities will be obligated to pay only for those services and/or equipment that they select and that they are not responsible for paying for the services and/or equipment selected by ETCOG or for paying for everything under the contract.

4.24 MAINTENANCE

Maintenance required for equipment proposed should be available in the ETCOG general area by a manufacturer authorized maintenance facility. Costs for this service shall be shown on the pricing/delivery information. If such providers are outside of the ETCOG area, the travel distance and means to Kilgore, TX must be specified. If ETCOG opts to include maintenance, it shall be so stated in the contract and said cost will be included. Service will commence only upon expiration of the required one year warranty, and should be priced accordingly.

4.25 CONTRACT OBLIGATION

ETCOG must award and must sign the contract before it becomes binding on ETCOG or the Respondent. Department heads are NOT authorized to sign agreements for ETCOG. Only the Executive Director, after formal approval by the ETCOG Board of Managers, is authorized to sign agreements from this RFP for ETCOG. Binding agreements shall remain in effect until all products and/or services covered by this purchase have been satisfactorily delivered and accepted.

4.26 TITLE TRANSFER

Title and risk of loss of goods shall not pass to ETCOG until ETCOG actually receives and takes possession of the goods at the point or points of delivery. Receiving times may vary with the using department. Generally, deliveries may be made between 8:30 a.m. and 4:00 p.m., Monday through Friday. Respondents are advised to consult the using department for instructions. The place of delivery shall be shown under the "Special Requirements/Instructions" section of this proposal and/or on the purchase order as a "Deliver To:" address.

4.27 WARRANTIES

Respondents shall furnish all data pertinent to warranties or guarantees which may apply to items in the proposal. Respondents may not limit or exclude any implied warranties. Respondent warrants that products sold to ETCOG shall conform to the standards established by the U.S. Department of Labor under the Occupational Safety and Health Act of 1970. In the event product does not conform to OSHA standards, where applicable, ETCOG may return the product for correction or replacement at the Respondent's expense. If Respondent fails to make the appropriate correction within a reasonable time, ETCOG may correct at the Respondent's expense.

4.28 DELIVERY

The successful Respondent shall not deliver products or provide services without a signed agreement by the Executive Director of ETCOG. The fastest, most reasonable delivery time shall be indicated by the Respondent in the proper place on the proposal document. Any special information concerning delivery should also be included, on a separate sheet, if necessary. All items shall be shipped F.O.B. INSIDE DELIVERY unless otherwise stated in the specifications. This shall be understood to include bringing merchandise to the appropriate room or place designated by the using department. Every tender or delivery of goods must fully comply with all provisions of these requirements and the specifications including time, delivery, and quality. Nonconformance shall constitute a breach, which must be rectified prior to expiration of the time for performance. Failure to rectify within the performance period will be considered cause to reject future deliveries and cancellation of the contract by ETCOG without prejudice to other remedies provided by law. Where delivery times are critical, ETCOG reserves the right to award accordingly.

4.29 CONTRACT RENEWALS

Renewals may be made ONLY by written agreement between ETCOG and the Respondent. Any price escalations are limited to those stated by the Respondent in the original proposal.

4.30 INVOICES AND PAYMENTS

Respondents shall submit invoices in duplicate on each purchase release after each delivery, indicating the purchase order number. Invoices must be itemized. Any invoice, which cannot be verified by the contract price and/or is otherwise incorrect, will be returned to the Respondent for correction. Under term contracts, when multiple deliveries and/or services are required, the Respondent may invoice following each delivery and ETCOG will pay on invoice. Contracts providing for a monthly charge will be billed and paid on a monthly basis only. Invoicing and payments must, at minimum, be in accordance with the Texas Prompt Payment Act.

4.31 TERMINATION

ETCOG reserves the right to terminate the contract for default if Respondent (Seller) breaches any of the terms therein, including warranties of Respondent or if the Respondent becomes insolvent or commits acts of bankruptcy. Such right of termination is in addition to, and not in lieu of, any other remedies which ETCOG may have in law or equity. Default may be construed as, but not limited to, failure to deliver the proper goods and/or services within the proper amount of time, and/or to properly perform any and all services required to ETCOG's satisfaction, and/or to meet all other obligations and requirements. ETCOG may terminate the contract without cause upon thirty days written notice to Respondent unless otherwise specified.

4.32 RECYCLED MATERIALS

ETCOG encourages the use of products made of recycled materials and shall give preference in purchasing to products made of recycled materials if the products meet applicable specifications as to quantity and quality. ETCOG will be the sole judge in determining product preference application.

4.33 SCANNED OR RE-TYPED RESPONSE

If in its response, Respondent either electronically scans, re-types, or in some way reproduces ETCOG's published proposal package, then in the event of any conflict between the terms and provisions of ETCOG's published proposal package, or any portion thereof, and the terms and provisions of the response made by Respondent, ETCOG's proposal package *as published* shall control. Furthermore, if an alteration of any kind to ETCOG's published proposal package is only discovered after the contract is executed and is or is not being performed, the contract is subject to immediate cancellation.

4.34 CONTRACT TERM AND OPTION TO EXTEND

Proposals must be for an initial contract term not less than three years nor more than five years with the options to extend the contract for two, two-year renewals.

Respondents' proposals must indicate the ability to agree to reasonable liquidated damages provisions to address damages for noncompliance with deliverables and quality of service commitments.

The balance of this page is intentionally left blank.

5. IP NETWORK

The proposed ETCOG IP network must be private, robust, scalable, secure, and sustainable. The response should describe how the proposed solution meets each of these goals. Respondents must propose a network solution for all sites listed herein.

5.1 PROJECT GOALS

ETCOG's long-term goal is the migration of 9-1-1 and public safety services to a private, reliable, secure, efficient, and cost effective IP network infrastructure using proven off-the-shelf technologies. The present project, a managed IP network to interconnect the ETCOG office, PSAPs, and police departments, is the first step towards that goal.

Since ultimately this infrastructure will carry 9-1-1 voice traffic to the PSAPs (among other services) the new IP-enabled network will ultimately need to be redundant and diverse in order to achieve the required reliability. Individual circuit, hardware, or firmware failures must not disrupt normal IP communication. There must be no single-point of failure in an IP infrastructure that carries "live" 9-1-1 calls.

Several years of planning and work will be needed to consolidate, update, or replace existing PSAP equipment and install suitable gateways and other devices and functions before this new IP infrastructure transports a substantial portion of the ETCOG 9-1-1 traffic. In the meantime, ETCOG incurs the cost of operating both the traditional 9-1-1 network and the new IP infrastructure during a time of economic stress and shrinking budgets.

Therefore ETCOG is employing a "staged" approach to the IP network implementation. The initial deployment will not implement all aspects of redundancy and diversity at all sites, until such time as the migration to the IP network requires these features. Even so, the IP network will be available for a number of uses, such as improved call-transfer capability, consolidation and sharing of public safety resources, and distribution of GIS data and updates. These uses will justify the cost of the new network and prepare the way for the realization of the long-term goal.

5.2 GENERAL TECHNICAL REQUIREMENTS

ETCOG does not proscribe how Respondents should implement the IP network. ETCOG's view of the network is at OSI Layer-3, that is, the delivery of IP packets between nodes on the network. From ETCOG's perspective, and in the absence of security policies specified by ETCOG, the network must deliver IP packets from any IP address to any other IP address among any and all connected sites.

Respondents may select any Layer-1 (copper, fiber, wireless, etc.) and any Layer-2 (HDLC, frame-relay, ATM, MPLS, etc.) technologies, in any combination and arrangement, that will deliver the most cost effective solution which will meet the requirements of the RFP. Respondents must provide, directly or through subcontractors, the Layer-1/Layer-2 facilities, as may be required, to interconnect to the specified sites.

Respondents must disclose the Layer-1 and Layer-2 technologies and topologies that they intend to deploy by providing network diagram(s) and text that show and explain these implementation details. Diagrams need not, and likely should not, be complete network diagrams showing all network sites. Rather, they should display enough information about the core network and about each unique type of site connection so that the topology and design of Layers 1, 2, and 3 are clear. The diagrams and narrative must provide sufficient information so technical reviewers can identify how the design meets the requirements and intent of this RFP. The drawings or narrative must convey all points of interconnection (POIs) and/or hub locations.

In any case the Layer 3 IP service must meet the service level requirements specified in Appendix B.

A brief discussion of the rationale for the network topology and the Layer 1 and Layer 2 design, and listing the advantages of the design, is recommended.

Any potential single points of failure in this initial deployment must be noted on the drawings or in the narrative.

Both hard copies and soft copies must be included in the response. Drawing must be .pdf or Microsoft Visio files.

5.2.1 Open Standards

The proposed network must be based on open standards, such as IEEE 802 at ISO Layer-2, and IP and Transmission Control Protocol (TCP), as defined by the IETF in applicable RFCs, at ISO Layer-3 and above.

Any and all protocols that run on top of or that use IP for transmission must be transported over the proposed network. No protocol or use of the IP network may be blocked or prevented by the network provider, unless in compliance with authorized ETCOG security policies.

Respondents must reveal any use of proprietary standards or protocols in their proposed solution, or state that they fully comply with this requirement. Any limitations, whether technological or philosophical, must be revealed.

5.2.2 Scalability

The overall design must scale to the eventual goal of a high-availability, voice-ready IP network interconnecting all the specified sites, redundantly interconnect additional sites, and redundantly interconnect other (separate) public safety IP networks.

The proposed network will include a strategy for expected growth over the next five to seven years. The design should plan for a doubling of the number of connected sites, and interconnections to as many as six additional public safety IP networks. The design must accommodate this goal without wholesale replacement, fork lift upgrades, or excessive non-incremental cost.

Respondents must demonstrate, though the diagrams, narrative, and pricing, how this goal can be realized with the proposed network design. This narrative should explain changes or upgrades to proposed components of the network that would be required to accomplish this level of expansion.

5.2.3 Architectural Survivability

The core network and the redundantly connected sites must be able to survive the total destruction, such as by fire or flood, of any one core network site, such as a switching center, data center, or POI site.

The proposed network solution and supporting hardware must be designed so that any one failure of any one circuit or equipment shall not result in a total network failure, but only the loss of connectivity associated with that circuit or equipment. For sites listed as “redundant,” loss of one such connection must not interrupt service to that site.

The proposed network should incorporate service provider and/or facility diversity wherever it is economically reasonable to do so. Where economically available, the network core solution and redundantly connected sites should include physically diverse routes and physically diverse building entrances. Any network elements that are not provisioned with physical diversity must be revealed and explained in the proposal.

Once full redundancy has been implemented to all sites, the proposed network should be designed to provide “five nines” availability to all sites as measured monthly. The service level agreements (SLAs) will specify the performance requirements for the network as actually deployed at any time.

Respondents should support claims of reliability by including known or projected network reliability statistics or other scientific data which supports those assertions. Respondents should also describe obstacles and risks to achieving high availability in their proposed solution.

5.2.4 Network Upgrades and Maintenance

It is a requirement that the proposed core network and redundantly connected sites not require down time for planned maintenance. It is acceptable that individual components or elements have down time for planned maintenance; however, the Respondent must provide an explanation of how the proposed solution will remain operational when such planned maintenance is performed. Note that a fully redundant design together with appropriate standard operation procedures (SOPs) for maintenance should meet this requirement.

5.2.5 Bandwidth

ETCOG will require the network provide, as a minimum, the bandwidth listed in 2.4.1.3. The bandwidths specified represent the minimal initial requirements.

The proposed solution must support a growth in bandwidth at each site to at least four times the initial requirements by adding facilities or using faster facilities, but without replacing major components such as core or on-site routers. In the alternative, Respondents must provide pricing for all the equipment upgrades required to the proposal to obtain the conceptual bandwidth.

The bandwidth requirements in 2.4.1.3 are for a fully functioning network with redundant connections in service. The failure of a redundant link may result in a loss of up to 50 percent of the specified minimum bandwidth to the effected site(s). This loss of bandwidth is allowable under the terms of the RFP.

5.2.6 Network - ETCOG Interface

At each redundant network site, the demarcation interface to ETCOG Local Area Networks (LANs) shall be two redundant 100-Megabit or faster UTP Ethernet ports. The Respondent should list and describe the Ethernet port fail-over scheme proposed.

The fail-over scheme should be one that is widely used in the industry and that complies with open standards. An example of an acceptable fail-over scheme is “Virtual Router Redundancy Protocol” (VRRP) version 2.0 as defined in RFC-3768. The latest version of VRRP, version 3.0, has recently been published in RFC-5798, in March 2010.

Non-redundant sites may utilize a single 100-Megabit or faster UTP Ethernet port.

5.2.7 IP addressing

The proposed network must support both IP Version 4 (IPv4) and IP Version 6 (IPv6) addressing at the network site demarcations into ETCOG LANs.

The successful Respondent will be required to obtain a block of IPv6 addresses from the Texas Commission on State Emergency Communications (CSEC), in anticipation of future interconnection with other regional and state-level ESInets.

The Respondent will be responsible for administering this block of IPv6 addresses in accordance with policies established by ETCOG officials, including making ample sub-allocations to PSAPs and holding allocations in reserve for other sites that may interconnect with the ETCOG public safety IP network.

The core network, including links to routers located at ETCOG sites, must be provisioned with IPv6 addresses from the allocated block. The proposed network shall be statically addressed at all major network interfaces, such as at router interfaces. A “loopback” interface with a unique static IPv6 address must be assigned to each network element that is capable of IP administration, such as a router, switch, or server.

Respondents must describe their IP address space administrative procedures, and provide information or requirements for an authorized entity in the ETCOG region to obtain an address space allocation.

The successful Respondent will be required to work with entities that presently implement only IPv4 addresses to assign a suitable IPv4 address to their Ethernet demark connection, to map their IPv4 address space into IPv6, and to provide other support as needed to assist with IPv4 address issues. Note that while the Respondent will not be required to make changes in entity IP networks that are outside the scope of this RFP, the Respondent will be required to fully cooperate with those entities, such as to provide information, perform configuration changes in edge network routers, or change entries in core domain name system (DNS) services, and generally go the "extra mile" to assist entities to utilize the ETCOG IP network to the fullest extent possible.

The cost of providing IP addressing services must be listed in the network management component of the pricing.

5.2.8 IP Routing

The IP network must implement a dynamic interior gateway IP routing protocol. ETCOG requests Open Shortest Path First (OSPF) as defined in IETF RFCs and as commonly implemented in the industry. However, vendors may present other solutions for the consideration of ETCOG, provided the solution is open and is supported on Linux, Microsoft, and Unix hosts.

The IP routing protocol must provide for the delivery of IP packets from any IP address to any other IP address in the ETCOG network, or in any connected IP network, or in any reachable IP network through a connected IP network.

The selected Respondent will be required to configure the ETCOG IP network and to work with the operators of interconnected IP networks to resolve IP routing problems as a feature of the supplied service.

The IP routing protocol must be set up to provide automatic IP rerouting in the event of a failure of any network facility or component, and in the presence of a redundant path around the failure point.

Of particular concern with dynamic IP rerouting is the behavior of the network in the event of a "flapping" circuit or equipment, that is, a device or facility that is rapidly transitioning between an operative and an inoperative state and back again. The dynamic routing protocol must be configured (tuned) to prevent instability of the network and to prevent serious loss of bandwidth due to routing table updates or other deleterious behavior in the presence of a flapping device or other such intermittent problem, while still providing automatic rerouting as quickly as is reasonably possible.

Incorrect configuration or changes of IP routing represent a serious threat to the availability of an IP network. The Respondent must describe their change management procedure with respect to network changes and updates, and explain how they mitigate the risk of human error in managing IP routing in the proposed network.

The Respondent should provide a short narrative describing the IP routing protocol implementation. This narrative should also describe how the network will respond to various failure scenarios and how route instability in the network will be avoided.

IP routing topics will likely be discussion points if a Respondent is invited to make a presentation to the RFP evaluation committee.

5.2.9 Quality of Service

The proposed network must implement a QoS function that can assure timely delivery of RTP packets even in the presence of network congestion from other non-real-time protocols, up to the limit of the available bandwidth.

The QoS system must also be able to prioritize other non-real time traffic, such as SIP traffic, if needed.

QoS support for RTP streams must be configured into the network. The design should minimize excessive latency and jitter. Refer to Appendix B for specified service levels.

The QoS scheme proposed should insure that a specific RTP session does not "share" bandwidth on redundant links. This requirement is to insure that RTP packets in User Datagram Protocol (UDP) stream do not arrive at the destination out-of-sequence should the redundant links have considerably different latencies. The proposal should include a brief narrative describing how the proposed system avoids this possible source of degradation of voice quality.

Interconnections with other ESInets may require cooperation to insure QoS is maintained for traffic traversing these network-to-network interfaces. The successful Respondent will be required to work cooperatively with the operators of interconnecting network to resolve QoS and voice quality issues, should they arise, regardless of the source of the issue, as part of the network management component of the pricing.

The development of new protocols or technologies may require modification or changes to the QoS scheme. Respondents should address their position and strategy on dealing with QoS changes that may be required in the future.

It is ETCOG's desire to understand how the proposed solution will provide the required QoS functionality. Respondents must provide an overview of how they prioritize traffic across the network. The narrative should discuss topics such as what network elements make QoS decisions, how priority packets are identified, how network elements handle congestion scenarios, and what mechanism(s) is used to provide priority to media streams. Any interaction between the QoS implementation, IP routing, or other protocols should be explained.

Proposals should explain what mechanisms or strategies, if any, are present in the proposed network to mitigate this potential problem.

5.2.10 Network Address Translation (NAT)

The use of NAT within the proposed network is highly discouraged.

That said, NAT capability at points of interconnection with other IP networks may be required in order to resolve possible IP addressing issues. But review the requirements in 5.2.7, which are intended to reduce the need for NAT.

NAT presents special problems for the reliable implementation of SIP and RTP streams that traverse the NAT device. Vendors that propose the use of NAT must be prepared to demonstrate their understanding of the SIP/NAT problem, and explain how they intend to mitigate any issues that might arise. ETCOG may require contract language to assure reliable operation of the network for its intended purposes in the presence of NAT.

5.3 AUXILIARY IP NETWORKS

Other IP networks may presently exist or will be constructed in the near future, for many purposes. For example, ETCOG currently leases an IP network that connects many of these same PSAP sites. This non-redundant IP network provides mapping and GIS updates to the PSAPs. Wideband public Internet is also present at some PSAP sites. For purposes of this RFP, such networks are lumped under the heading "auxiliary" IP networks.

The service levels associated with such existing IP networks is not determined, and their suitability for the purposes of this RFP is unknown. For example, the Internet provides no QoS, no guaranteed service levels, security, or other

features requested in this RFP. Generally speaking, the use of the public Internet, in itself, is not a viable alternative for a public safety IP network.

Never-the-less, even in the absence of QoS and other features, many people successfully use Skype and other VoIP services over the Internet on a regular basis with few, if any, serious issues, or with only brief interruptions in the quality of the service.

ETCOG wishes the option of leveraging auxiliary IP networks to mitigate outages, supplement bandwidth, or improve the survivability of the public safety IP network.

Respondents are requested to provide the option of an additional Ethernet interface at specific sites that can be used to interconnect to one of these auxiliary IP networks. A static IP address from the auxiliary network's address space is assigned to this interface for the purpose of creating an encrypted tunnel or Virtual Private Network (VPN) between the two sites. This foreign IP address is not routed and is not addressable from the ETCOG IP network, or vice versa.

The public safety network can then assign its own IP addresses to the tunnel interfaces, and the QoS system can route low-priority traffic via the tunnel.

The encrypted tunnel is a virtual point-to-point IP connection for the public safety IP network, which uses the auxiliary network as transport, but which otherwise cannot and does not interconnect or interoperate with the auxiliary network.

5.4 NETWORK MONITORING

The transport network must be monitored on a 24x7 basis. The Respondent must be equipped with a NOC staffed to support 24x7 restoral or mitigation of incidents. The Respondent must provide a 24x7 toll free number accessible to ETCOG-authorized personnel, as determined by ETCOG.

The use of the network-provider monitoring system does not preclude ETCOG from installing and using its own monitoring system for remotely monitoring PSAP equipment, using the IP network for remote environmental monitoring of connected sites, or other such applications.

ETCOG will require pricing for a fully-managed network to meet public safety best practices.

The monitoring of the network and associated reporting must encompass the following areas:

5.4.1 Network Fault Management

Fault management will detect, log, and notify the network operator, and depending on severity and policy, the ETCOG staff, of IP network problems, such as failed circuits, equipment, or network functions. If the failure immediately corrects itself, notification is not required, but all events must be logged and reported.

5.4.2 Network Performance Management

Performance management will measure the variables that affect network performance. Network performance reports describing overall network usage, congestion events, outages, and other such data will be required on a monthly basis.

Network performance management data access is required from all manageable IP devices as specified in contractual agreements. Network performance management and reports must be priced as an itemized option.

Respondents should provide detailed descriptions of what performance data will be collected and how this data will be logged and reported, including such details as how alarm thresholds are determined,

All IP manageable network hardware shall support the SNMPv3 specification for performance management via standard management information base (MIB) objects forwarded to or extracted by any ETCOG designee.

5.4.3 Information Retrieval

Respondents must describe how their proposed solution retrieves information for reporting purposes. The description should include comments regarding any requirements made upon ETCOG for this feature.

5.5 NETWORK MANAGEMENT

5.5.1 Network Configuration Management

Respondents must describe the process and/or SOP that they use for making changes to the network configuration, such as: adding a connection, re-provisioning a circuit, or changing a QoS priority. The description should mention or describe procedures such as how proposed changes are planned, authorized, authored, reviewed, noticed, implemented, tested, backed out, and backed up, and the personnel involved. The role and any requirements upon ETCOG in this process are especially important. ETCOG views this process as very important to realizing “five nines” network availability.

5.5.2 Configuration Restoration

Respondents must describe their capability to automatically or routinely backup configuration data, and the process and conditions used to restore the configuration of network elements such as routers or switches, should the need arise.

5.5.3 Root Cause Analysis (RCA)

For major outages, the network provider should provide ETCOG staff with a RCA within five business days; and for minor outages, provide an RCA upon request. Respondents should describe the tools and techniques at their disposal to perform troubleshooting and post-event analysis.

5.5.4 Preventative Maintenance

Respondent should train ETCOG technical personnel to perform preventative maintenance. The provider should include preventative maintenance activities that will be included as part of a maintenance contract. This should address how preventative maintenance is handled, as well as the frequency of preventative maintenance activities. The provider should use support logs to drive the development of solutions to recurring issues and follow industry best practices.

5.5.5 Scheduled Maintenance

Respondent shall train ETCOG technical personnel to perform scheduled maintenance. Any maintenance by Respondent, including upgrades to the network, must be coordinated in advance with ETCOG and conducted in accordance with a mutually disclosed SOP. The network provider should make all attempts to assure that a remote location and its designated back up are not affected at the same time.

5.5.6 Security Monitoring and Management

Security Monitoring and Management should be quoted as an option. Respondents quoting this option should have knowledge of security standards found in documents such as, but not limited to, NENA NG-SEC , NENA i3 Technical Requirements Document 08-751 and NENA Functional and Interface Standards for NG9-1-1 Version 1 (i3).

The Respondent’s security management solution must control access to network resources according to public safety network security guidelines to prevent sabotage (intentional or unintentional) and the compromise of sensitive

information. Security management must use public safety network security standards to monitor users logging into the network resources and refuse access to those who enter inappropriate access codes. The proposed IP-enabled network should support standard security policies that may include the use of anti-virus software, virtual local area networks (VLANs), VPNs, and secure sockets layer protocols.

Furthermore, any system that connects to an IP-enabled network should be required to comply with standards, including the standards and demonstrate compliance through an initial and recurring audit.

Although this will start as a "closed" network solution, security policies, processes, and procedures must be designed in such a method so that when ETCOG chooses to be part of an ESInet that the proposed security components will not require "fork lift" replacement.

Within this response, explain how the proposed solution meets this requirement.

5.6 TRANSIENT VOLTAGE SURGE SUPPRESSION (TVSS)

Secondary TVSS shall be installed in addition to primary protection, typically on facilities such as punch down blocks, or via plug-in modules, and are used to protect the equipment from voltages that may have been introduced into the sites from utility and communication facilities.

All copper pairs entering the building must be provided with secondary TVSS protection. TVSS devices must protect all incoming and outgoing equipped ports that are, or could be connected to wireline or wireless facilities, including Central Office (CO) Plain Old Telephone Service (POTS), 9-1-1 trunks, T1/DS1 facilities, Ethernet, or ETCOG owned CPE and ETCOG owned facilities.

The Respondent is required to include an installation kit including all ground bars and ground wiring for installation.

The secondary TVSS devices must list a clamping voltage of 250 volts (.5kV) or less and operate in < 10 nanoseconds. The device shall meet UL497A requirements and must have an operational indicator to alert maintenance personnel that the device has been utilized, failed, or that the circuit no longer is protected. The secondary TVSS must not degrade the audio signaling and must have a minimum of one year manufacturer's warranty. Example products might be: UltraLinx UP3P 66 Block protection, or a MLLT1 SureGate from ITWLinx for the T1 lines.

5.7 SPARES

Respondents should describe their spares program, such as stocking levels, stocking locations, and the time required for a field technician already on site to access a spare. The role of ETCOG, if any, in spare stocking or access must be explained.

5.8 NEW ORIGINAL EQUIPMENT MANUFACTURER (OEM) EQUIPMENT

Only new equipment will be considered. Refurbished or used equipment shall not be considered as part of the proposed solution. ETCOG requires that proposed hardware be in current manufacture. If a proposed device goes into end-of-life within the contract period, its equivalent or better current manufacture must be installed. Included in the proposed response shall be the life cycle of the proposed solution or equipment.

5.9 SERVICE LEVEL AGREEMENTS

Required network SLAs can be found in Appendix B. Respondents must submit a response to the requested SLAs. The Respondent must measure and provide reports on the network performance against the SLAs on a monthly basis. For any circuit downtime, outages, or interruptions, the Respondent must provide information in their monthly reports describing the degradation in service, or outage, including the root cause. The report will provide a plan for preventing similar occurrences in the future. Trend data must be included in the report, including the previous two months performance summary.

5.10 NETWORK AND ACCEPTANCE TESTING PROCESS

Respondent must include complete and detailed network test and acceptance test processes that include, but are not limited to, application testing, integration testing, interface testing, and production testing. The awarded Respondent must be willing to work with ETCOG regarding all areas of the test plan and execution.

The balance of this page is intentionally left blank.

6. EMERGENCY TELEPHONE SYSTEM

Proposals for an Emergency Telephone System for the Longview Police Department, 302 W Cotton Street, Longview, TX, are solicited.

All requirements, terms and conditions of this RFP as outlined in Sections 1, 2, 3, and 4 apply to this section.

Respondents must be aware that Longview Police Department on-site workers are required to be finger printed and background checked. Longview reserves the right to refuse any worker whose background check does not satisfy Longview's criteria.

All contact with Longview Police Department with respect to the Emergency Telephone System procurement should be directed to:

Mailing and Physical Address

Attention: Ms. Sally Rees
Manager
Public Safety Communications
P.O. Box 1952
302 W Cotton Street
Longview, TX 75606
903-237-1139
Srees@LongviewTexas.gov

Respondents are highly encouraged to conduct a pre-proposal site walkthrough. The PSAP greatly prefers these visits occur on September 28th, either before or after the pre-proposal vendor meeting in Kilgore. Please send an email in advance indicating the planned time of the visit to Sally Rees, Manager, srees@LongviewTexas.gov.

Respondents requiring an on-site visit on other dates must contact Sally Rees in advance for an appointment.

6.1 CURRENT LONGVIEW CPE CONFIGURATION

The present system, entirely located within the Longview Police Department building, consists of a Positron Lifeline ANI/ALI controller interconnected with an Avaya G3 PBX which provides the switching function and some line terminations. This PBX is dedicated to the emergency telephone system functionality, that is, it does not support any other extensions or trunks beyond those listed here.

The LifeLine / PBX system supports eleven Power 9-1-1 V5.1 answering positions, five of which are primary dedicated 9-1-1 call taker positions, five of which are located at dispatcher positions and used as backup positions and for call overflow, and one position which is used for training and testing.

The Lifeline terminates eight analog CAMA 9-1-1 trunks, four of which are dedicated to wireline calls and four of which are dedicated to wireless incoming calls. These trunks appear on all the answering positions as in a key system; no ACD functions are implemented. Any position can answer any trunk.

The system also terminates twenty analog POTS lines, five of which are used for call transfers, five of which are connected to gateways to the city's Cisco UCM VoIP PBX system and appear as extensions (in a ring group) on that

system, five lines that are in a ring group and that can be answered or selected from any Power workstations, and five that are dedicated, one to each of the five primary 9-1-1 answering positions.

The Lifeline also is connected to ten ringdown (PLPA-type) circuits, eight of which are connected to various positions in an area fire department, one connected to the Emergency Operations Center (EOC), and one connected to the Gregg County Sheriff's Office.

There are two PBX extension lines that connect to telephones located in the front lobby and hallway of the same building.

The Lifeline terminates two traditional ALI data circuits to a remote ALI database server operated by AT&T.

The Lifeline also provides an RS-232 Serial Data CAD interface, which is connected to a Tiburon Command CAD V2.3.1 system. An upgrade to Tiburon Command CAD V2.6 is expected in the near future.

The Lifeline interfaces to a Higher Ground recording system and a Spectracom Netclock time server.

6.2 GENERAL TECHNICAL REQUIREMENTS

At a minimum, proposals must replace the LifeLine,Avaya PBX, and the present Power 9-1-1 answering positions. The answering position count and usage will remain unchanged.

The replacement system must include Management Information System (MIS) functions that are able to generate standard tabular and graphical reports, including:

- Emergency call traffic counts, by hour, day, week, and month, and by trunk or trunk group
- Administrative call traffic counts, by hour, day, week, and month, by line and by position
- Average call answer time, call duration, and call hold times, by operator
- Abandoned calls
- User-defined reports using a reporting tool

6.2.1 System Sizing and Functions

The sizing of the replacement system must equal or exceed the present installation. The system must be able to incrementally accommodate up to a 25 percent growth in answering positions, lines, trunks, and traffic without replacement of major and/or centralized components, or excessive non-incremental cost, over the next 3-5 years.

The replacement system must provide the circuit terminations of the existing system. It must faithfully reproduce the functionality of existing system, and provide the functionally listed in appendix D. The replacement system must also provide IP and NG9-1-1 capabilities as listed in the requirements in this section. System redundancy shall be built into the design of the system so that there shall be no single point of failure.

6.2.2 Standards Requirements

The proposed ETS must comply with NENA recommended Generic Standards for PSAP CPE, as outlined in NENA document 04-001. Any exceptions to these generic recommendations must be listed in the response.

The proposed ETS must also be compatible with the intent and purpose of the current NENA i3 draft.

The Respondent must demonstrate philosophical and technical commitment to the NENA i3 standard as it is finally adopted, and provide a roadmap and a timeline for providing upgrades, with projected costs, for NENA i3 compliance as the standard becomes available.

6.2.3 Required NG9-1-1 Features

Not-withstanding 6.2.2, the following NENA "i3-like" features are explicitly required:

> Session Initiation Protocol (SIP) compatible with full compliance to RFC 3261. Respondents must explicitly state any and all exceptions to RFC 3261
>
> Reception of location data using the PIDF-LO data format as defined in RFC 4119, and encapsulated in the SIP messages that set up the call to the PSAP per RFC 3261. (SIP location-by-value)
>
> Three-party call transfer capabilities compatible with RFC 3261, including the ability to forward SIP encapsulated location data via the PIDF-LO to the transfer target, and the ability of the transferor to drop out of the three-party call and leave the caller and transfer target connected. For this requirement it may be assumed that the SIP call origination device and the transfer target are fully RFC 3261 compliant.
> Voice-over-IP (VoIP) Real-time Transport Protocol (RTP) using the G.711 codec.
>
> Support for IPv6 addressing. The system IP interfaces, the SIP protocol implementation, and the VoIP RTP implementation must also support IPv6 addressing, or the Respondent must show how SIP and RTP support for IPv6 will be provided no later than July 1st, 2012.

The proposed system must present any call received via SIP with PIDF-LO formatted and encapsulated location data to the call taker on the same displays and formats as for a legacy 9-1-1 call with a normal ALI response.

Respondents must discuss how they will comply with each of the requirements of this section, and list any and all limitations imposed by their solutions on these requirements, if any.

6.2.4 Call Transfer Interoperability over IP

Of particular interest to Longview Police Department is the ability to transfer 9-1-1 calls, or receive transferred 9-1-1 calls, with accompanying ALI data, to or from the ETCOG PSAPs over the IP network that is the subject of this RFP.

The ETCOG PSAPs all use PlantCML Vesta Pallas CPE running V2.7 or later software. Per the manufacturer, this equipment and software version is able to transfer calls via IP and SIP amongst like Vesta Pallas systems. However, the ALI data is passed using a PlantCML proprietary protocol.

The proposed system must provide the same or similar functionality to enable call transfer interoperability with PlantCML Patriot and Positron VIPER CPE as well.

Respondents must discuss their ability to supply a solution compatible with this environment, with timelines and costs. A solution that can gateway between the proprietary PlantCML protocol and the SIP encapsulated PDIF-LO as required in 6.2.3 above is acceptable.

6.2.5 System Monitoring and Notification

The proposed system must self-monitor in real-time for critical and major circuit or internal failures. The system must be equipped with an automatic notification system that notifies designated Longview Police Department personnel of such critical or major alarms. The preferred notification system includes e-mail, voice call / voice-mail, or SMS text messaging to designated mobile phone numbers.

Respondents should disclose the availability and features for real-time NOC monitoring of the proposed CPE equipment. This can be a CPE vendor-operated 24/7/365 monitoring service, or, if the Respondent is also proposing an IP network in response to this RFP, a service of the IP network NOC. If available, the Respondent must provide itemized pricing for this service, along with a clear narrative of exactly what services the NOC provides to Longview Police Department.

6.3 CPE PRICING

Each CPE Element must have separate pricing. Core elements of the CPE must have separate pricing, including separation of pricing of hardware and software.

6.3.1.1 Cost Proposal

This section is intended to provide itemized costs for the Longview CPE. Respondents interested in submitting a proposal must provide details that illustrate how the Respondent plans to address the hardware, software, installation, implementation and maintenance of this project as specified. Respondents are responsible for all costs incurred in the development and submission of their proposals.

6.3.1.2 Cost Requirement

Costs must be provided for all the CPE elements. Respondents must provide separate detailed cost sheets for the CPE implementation phase and a soft copy in Microsoft Excel format with their proposal.

6.3.1.3 Cost Proposal Details

Any CPE server and software cost should be presented in the CPE pricing. Responses must also include a narrative on how the scalability of the CPE will be supported.

Respondents must also describe their plan to implement, to Longview CPE, new upgrades as they are developed in the future. Longview wants to assure that the Longview CPE products will remain reliable, efficient, cost effective and proven technologies. Respondents must submit detailed costs for the entire CPE project.

All costing data must be detailed in Microsoft Excel worksheets and delivered via soft copy and include the following minimum details:

- Detailed costs for the entire project; detailed paper worksheets need to be included and formatted
- Costs for all CPE, listing all individual components and elements and any other associated costs
- Incremental growth costs for hardware and software licenses; costs must include all associated components and elements
- Any CPE support, detailing all costs associated with supporting the CPE
- Total contract price per CPE category

Options as outlined herein

- Labor per hour for deletions, adds, moves and changes
- Labor per hour for change order activity, if utilized

6.3.1.4 Maintenance Pricing

Respondents must quote pricing fully managed CPE Services

6.3.1.5 Managed Services

Respondents responding to this RFP must detail the cost of their managed services, as well as the added value brought by their managed service offering.

Respondents are to be very specific as to exactly what managed services they are offering, to what systems/devices/functions, where the options are (end-to-end vs. piecemeal), itemized pricing, limitations, etc.

6.4 IMPLEMENTATION

Respondents must be aware of very limited space in both the equipment room and the call taker area of the Longview Police Department building. It will be a challenge to install the new system without excessively disrupting live operations. It will also be a challenge to operate both systems side-by-side until the cutover is accomplished.

Respondents must give careful planning to the installation, testing, training, and cutover process while operating within the constraints of space. Respondents should address these issues and make suggestions about how they will deal with these issues in their response.

6.4.1 Training

The respondent shall provide a comprehensive training program to assist Longview personnel to become proficient in the operation of all system components prior to system cutover. At minimum this shall include administer, supervisor and operator specific training. The respondent shall provide a draft of the training syllabus at least 30 days prior to the commencement of training for approval by Longview. Respondent shall accommodate all reasonable requests for modifications at no additional expense and conform to Longview's time schedule for class presentations.

6.4.2 Dual System Cutover

The Respondent shall provide a strategy, including timeframe, in this RFP, for providing dual service during cutover from current PSAP CPE to the proposed host, where applicable, and PSAP CPE. The cutover strategy shall provide a fallback provision if cutover to the proposed system is not fully functional within specified cutover window of time.

6.4.3 Pre-cutover Acceptance Testing

Proposals must include a pre-cutover acceptance testing plan strategy, in this RFP. Final details of the pre-cutover acceptance testing plan will be developed in the negotiation phase. Longview requires Respondent assurance that the cutover will occur flawlessly. Longview shall have the final say as to acceptability of all tests.

6.4.4 Certification

The awarded Respondent must perform their own acceptance testing prior to testing. Once the Respondent is satisfied that the system is as agreed upon, the awarded Respondent must certify that the installation is complete and meets all the agreed-upon requirements. This will serve as notification that Longview can begin acceptance testing.

6.4.5 Acceptance Testing

The awarded Respondent is required to provide post-cutover acceptance testing plans with respect to the following:

- Application tests
- Integration tests
- Interface tests
- Complete call processing
- Complete transfer processing

6.4.6 Fail-over Strategy

The Respondent shall provide a fail-over strategy. That fail-over strategy will provide for the ability of the CPE to be restored to "last working revision" within the maintenance window of time.

6.4.7 Production Test

Production tests occur when the system is live. Tests must last long enough to determine the system's integrity and reliability. The acceptance test will be successful if the system operates successfully in compliance with the system's performance specifications for a total of 30 consecutive days.

6.4.8 Post-cutover Final Acceptance Testing

The acceptance test will be successful if each of the levels of testing is successful and the system operates in compliance with the RFP and contract documents for a total of 30 consecutive days after the first day of productive use (go live).

Written notification will be furnished to the awarded Respondent if any item is determined unacceptable. The awarded Respondent will then have five business days to correct or replace the defective item and notify Longview that all such errors have been remedied. Longview will have three additional Longview business days to recommence the acceptance test.

This process will be repeated as necessary until the system meets the 30 consecutive day acceptance test.

6.4.9 Post-installation Follow-up

It shall be a requirement that a post-installation follow-up meeting take place between 45 and 60 days after system cutover to discuss open items, potential reconfigurations, and other issues.

6.4.10 PSAP Interface Wiring, Dmarc, Labeling, and Site Records Requirements

6.4.10.1 Demarc extension

The successful Respondent will be responsible for providing connectivity between any Telco demarcation point and the equipment being installed, as required.

6.4.10.2 Component Identification and Organization

The Respondent shall see that all routers, gateways, interface devices, equipment wiring, and terminations must be organized so that local personnel can clearly identify all network connections.

6.4.10.3 Common Labeling/Numbering Schemes

The Respondent shall see that all equipment, wiring, and terminations are required to be labeled in a fashion that relates to the common name for network connections rather than, or in addition to, proprietary or internal numbering schemes.

6.4.11 Drawings/Software

The Respondent shall provide at least one copy of an “as built” drawing in Visio or similar software that has been pre approved byLongview. All site-specific documentation and the site log must be presented to Longview in binders.

6.5 MIGRATION STRATEGY

The Respondent will provide a detailed migration strategy that will include documentation of design, conversion strategy, testing, and final steps to ensure effective migration processes and procedures are communicated and followed.

6.6 TRANSITION AND DEPLOYMENT ISSUES

The hosted CPE design allows for local information control and access while storing the data and services in core locations. The flexibility of an IP network allows for the development of contingency plans for major and minor events by creating a virtual PSAP environment.

The Respondent shall provide information on the ability to provide monthly progress reports that contain concise project information covering the activities relevant to:

- A clear and complete account of the work performed on each task
- An outline of the work to be performed during the next reporting period
- A bar chart showing the work accomplished by task versus the schedule of work of the contract and the cost schedule
- A discussion of any problems encountered or anticipated that might affect the completion of the contract within the time and fiscal constraints set forth in the contract, together with recommended solutions to such problems; or a comment that no problems were encountered
- A chart showing incremental costs per month for all services compared to the proposed timeline and the cost schedule
- Any other pertinent information, including an analysis
- Post-cutover assistance

7. CHAMPION EMS ANSWERING POSITIONS

Proposals for five answering positions for Champion EMS, 2201 South Mobberly, Longview, TX, are solicited. All requirements, terms and conditions of this RFP as outlined in Sections 1, 2, 3, and 4 apply to this section.

Champion EMS is a secondary PSAP site. Calls are transferred to Champion EMS from many ETCOG PSAPs. Today, the calls are received on regular POTS telephone lines. Today, ALI data is conveyed separately to Champion EMS via fax, telephone, radio or other external means.

7.1 SCOPE

Champion EMS desires to procure five fully-featured 9-1-1 answering positions that can accept transferred calls, display ALI, and perform transfers, conferencing, and the other functions of the primary PSAPs.

The proposed solution must be able to accept transferred calls from the ETCOG PSAPs using the PlantCML Vesta Pallas V2.7 or later software over the IP network that is also the subject of this RFP.

Per the manufacturer, the Vesta Palles equipment and software version is able to transfer calls via IP and SIP amongst like Vesta Pallas systems. However, the ALI data is passed over the IP network using a proprietary protocol.

Respondents may propose a complete stand-alone Emergency Telephone System (ETS) with its own ANI/ALI controller or equivalent functions.

Alternatively, Respondents may propose to supply PlantCML Vesta Pallas compatible answering positions. These answering positions would be hosted by the ANI/ALI controller located at Gregg County Sheriff's Office, and would communicate with that controller over the IP network that is the subject of this RFP.

7.2 GENERAL TECHINCAL REQUIREMENTS

Respondents must demonstrate and supply a solution compatible with the Vesta Pallas IP environment.

7.2.1 Standards Requirements

If a stand-alone ETS is proposed, the proposed ETS must comply with NENA recommended Generic Standards for PSAP CPE, as outlined in NENA document 04-001. Any exceptions to these generic recommendations must be listed in the response.

A proposed ETS must also be compatible with the intent and purpose of the current NENA i3 draft. The Respondent must demonstrate philosophical and technical commitment to the NENA i3 standard as finally adopted, and provide a roadmap and a timeline for providing, with projected costs, upgrades for NENA i3 compliance once the standard becomes available.

7.2.2 Required NG9-1-1 Features

Not-withstanding the requirements of 7.2.1, the following NENA "i3-like" features are explicitly required for a stand-alone ETS solution:

> Session Initiation Protocol (SIP) compatible with full compliance to RFC 3261. Respondents must explicitly state any and all exceptions to RFC 3261

Reception of location data using the PIDF-LO data format as defined in RFC 4119, and encapsulated in the SIP messages that set up the call to the PSAP per RFC 3261. (SIP location-by-value)

Three-party call transfer capabilities compatible with RFC 3261, including the ability to forward SIP encapsulated location data via the PIDF-LO to the transfer target, and the ability of the transferor to drop out of the three-party call and leave the caller and transfer target connected. For this requirement it may be assumed that the SIP call origination device and the transfer target are fully RFC 3261 compliant.

Voice-over-IP (VoIP) Real-time Transport Protocol (RTP) using the G.711 codec.

Support for IPv6 addressing. The system IP interfaces, the SIP protocol implementation, and the VoIP RTP implementation must also support IPv6 addressing, or the Respondent must show how SIP and RTP support for IPv6 will be provided no later than July 1st, 2012.

The proposed system must present any call received via SIP with PIDF-LO formatted and encapsulated location data to the call taker on the same displays and formats as for a legacy 9-1-1 call with a normal ALI response.

7.3 CPE PRICING

Each CPE Element must have separate pricing. Core elements of the CPE must have separate pricing, including separation of pricing of hardware and software.

7.3.1.1 Cost Proposal

This section is intended to provide itemized costs for the Champion EMS CPE. Respondents interested in submitting a proposal must provide details that illustrate how the Respondent plans to address the hardware, software, installation, implementation and maintenance of this project as specified. Respondents are responsible for all costs incurred in the development and submission of their proposals.

7.3.1.2 Cost Requirement

Costs must be provided for all the CPE elements at all locations. Respondents must provide separate detailed cost sheets for each CPE implementation phase and a soft copy in Microsoft Excel format with their proposal.

7.3.1.3 Cost Proposal Details

Any CPE server and software cost should be presented in the CPE pricing. If CPE is at multiple locations, each location must have pricing that is separate. Responses must also include a narrative on how the scalability of the CPE will be supported.

Respondents must also describe their plan to implement new upgrades as they are developed in the future. Champion EMS wants to assure that the proposed CPE products will remain reliable, efficient, cost effective and proven technologies. Respondents must submit detailed costs for the entire CPE project.

All costing data must be detailed in Microsoft Excel worksheets and delivered via soft copy and include the following minimum details:

- Detailed costs for the entire project; detailed paper worksheets need to be included and formatted
- Costs for all CPE, listing all individual components and elements and any other associated costs
- Incremental growth costs for hardware and software licenses; costs must include all associated components and elements
- Any CPE support, detailing all costs associated with supporting the CPE

- Total contract price per CPE category

Options as outlined herein

- Labor per hour for deletions, adds, moves and changes
- Labor per hour for change order activity, if utilized

7.3.1.4 Maintenance Pricing
Respondents must quote pricing fully managed CPE Services

7.3.1.5 Managed Services
Respondents responding to this RFP must detail the cost of their managed services, as well as the added value brought by their managed service offering.

Respondents are to be very specific as to exactly what managed services they are offering, to what systems/devices/functions, where the options are (end-to-end vs. piecemeal), itemized pricing, limitations, etc.

7.4 IMPLEMENTATION

7.4.1 System Installation
The Respondent shall provide a strategy, including timeframe, in this RFP, for CPE installation, accepting testing, and certification.

7.4.2 Pre-commissioning Acceptance Testing
Proposals must include a pre-commissioning acceptance testing plan strategy, in this RFP. Final details of the acceptance testing plan will be developed in the negotiation phase. Champion EMS requires Respondent assurance that the turn-up will occur flawlessly. Champion EMS should have the final say as to acceptability of all tests.

7.4.3 Certification
The awarded Respondent must perform acceptance testing prior to Champion EMS testing. Once the Respondent is satisfied that the system is as agreed upon, the awarded Respondent must certify that the installation is complete and meets all the agreed-upon requirements. This will serve as notification that Champion can begin acceptance testing.

7.4.4 Acceptance Testing
The awarded Respondent is required to provide post-cutover acceptance testing plans with respect to the following:

- Application tests
- Integration tests
- Interface tests
- Complete call processing
- Complete transfer processing

7.4.5 Fail-over Strategy
The Respondent shall provide a fail-over strategy. That fail-over strategy will provide for the ability of the CPE to be restored to “last working revision” within the maintenance window of time.

7.4.6 Production Test

Production tests occur when the system is live. Tests must last long enough to determine the system's integrity and reliability. The acceptance test will be successful if the system operates successfully in compliance with the system's performance specifications for a total of 30 consecutive days.

7.4.7 Post-cutover Final Acceptance Testing

The acceptance test will be successful if each of the levels of testing is successful and the system operates in compliance with the RFP and contract documents for a total of 30 consecutive days after the first day of productive use (go live).

Written notification will be furnished to the awarded Respondent if any item is determined unacceptable to Champion EMS. The awarded Respondent will then have five business days to correct or replace the defective item and notify Champion EMS that all such errors have been remedied. Champion EMS will have three additional Champion EMS business days to recommence the acceptance test.

This process will be repeated as necessary until the system meets the 30 consecutive day acceptance test.

7.4.8 Post-installation Follow-up

It shall be a requirement that a post-installation follow-up meeting take place between 45 and 60 days after system cutover to discuss open items, potential reconfigurations, and other issues.

7.4.9 Site Management

7.4.10 PSAP Interface Wiring, Dmarc, Labeling, and Site Records Requirements

7.4.10.1 Component Identification and Organization

The Respondent shall see that all routers, gateways, interface devices, equipment wiring, and terminations must be organized so that local personnel can clearly identify all network connections.

7.4.10.2 Common Labeling/Numbering Schemes

The Respondent shall see that all equipment, wiring, and terminations are required to be labeled in a fashion that relates to the common name for network connections rather than, or in addition to, proprietary or internal numbering schemes.

7.4.11 Drawings/Software

The Respondent shall provide at least one copy of an "as built" drawing in Visio or similar software that has been pre approved by ETCOG. In addition to this requirement, one copy must be made available to Longview or its representative. All site-specific documentation and the site log must be presented to Longview in binders.

7.5 TRANSITION AND DEPLOYMENT ISSUES

The hosted CPE design allows for local information control and access while storing the data and services in core locations. The flexibility of an IP network allows for the development of contingency plans for major and minor events by creating a virtual PSAP environment.

The Respondent shall provide information on the ability to provide monthly progress reports that contain concise project information covering the activities relevant to:

- A clear and complete account of the work performed on each task
- An outline of the work to be performed during the next reporting period

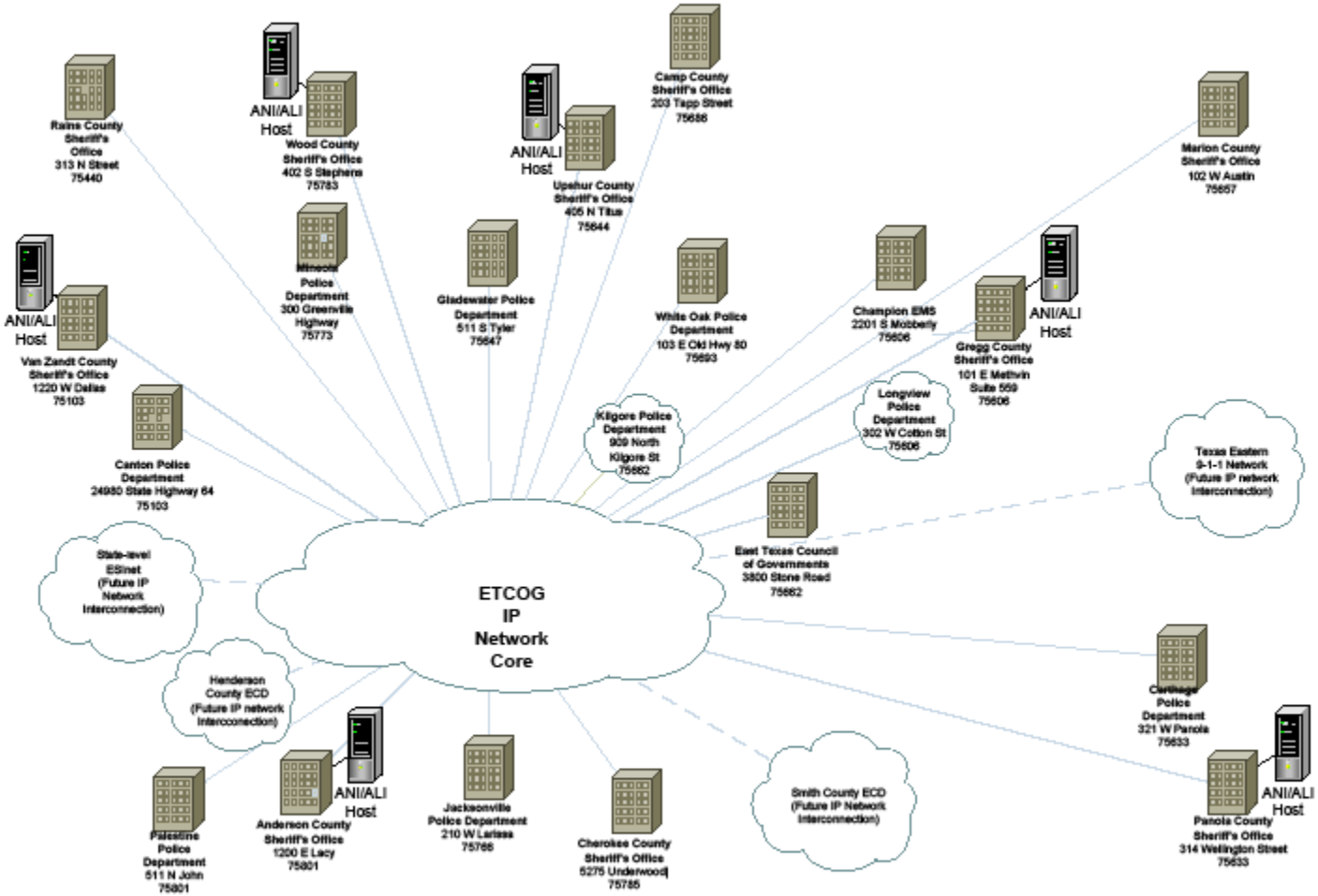
- A bar chart showing the work accomplished by task versus the schedule of work of the contract and the cost schedule
- A discussion of any problems encountered or anticipated that might affect the completion of the contract within the time and fiscal constraints set forth in the contract, together with recommended solutions to such problems; or a comment that no problems were encountered
- A chart showing incremental costs per month for all services compared to the proposed timeline and the cost schedule
- Any other pertinent information, including an analysis
- Post-cutover assistance

8. APPENDIX A – ETCOG CONCEPTUAL NETWORK DESIGN

The diagram on the next page is provided as an overview to illustrate logical network architecture only. It is not a specified physical network design or topology. ETCOG encourages Respondents to submit a proposed network design that is uniquely their own, and which delivers the identified performance and functionality most efficiently, cost effectively, and reliably for ETCOG.

The locations on the diagram are in very rough geographical relationship to each other, but not to scale. The heavier lines represent redundant, and diverse within economically reason, from the site to the core network.

The core network must be a highly available network incorporating redundancy and diversity between all POIs.



9. APPENDIX B – SERVICE LEVEL AGREEMENTS

This document provides requirements for IP network performance, and for providing network management reports and data.

9.1 NETWORK PERFORMANCE

The Respondent to this RFP is responsible for the performance of the proposed network in its entirety, except that performance over a virtual link provisioned via an auxiliary IP network is exempted from this section. All performance calculations must be based on the assumption that no virtual links provisioned on an auxiliary IP network are functioning.

Unless stated otherwise, calculations for the parameters in this section will be made assuming the network is operating normally, that is, all components, including redundant elements, are operating, and that the total traffic load on the network consumes at least 90 percent of the available bandwidth.

9.1.1 Voice Quality and Quality-of-Service

The proposed IP network must be capable of transporting VoIP using RTP encoded with G.711 codecs such that for 99 percent of all calls traversing the network, network users will perceive little, if any, audio quality degradation due to the quality of VoIP transport on the network.

At a minimum, the VoIP quality must be equivalent to the voice quality of a TDM call with a Mean Opinion Score (MOS) of at least 4. MOS is expressed as an integer ranging from 1 to 5, as follows:

- 5 - Perfect. Like face-to-face conversation or radio reception.
- 4 - Fair. Imperfections can be perceived, but sound still clear. This is (supposedly) the range for cell phones.
- 3 - Annoying.
- 2 - Very annoying. Nearly impossible to communicate.
- 1 - Impossible to communicate

Respondents must state the applicable network performance parameters (e.g. packet loss, jitter, latency) and metrics used to insure and measure the VoIP quality. However, meeting network latency, pack loss, or jitter specifications does not relieve the vendor from also meeting the VoIP quality requirement.

The QoS system must permit the Voice Quality criterion to be satisfied when the total RTP traffic load on the network is at least 50 percent of the total network bandwidth, and when the total IP traffic demand for the network exceeds 110 percent of the available network bandwidth for an interval of at least 30 seconds.

9.1.2 Network Latency

Respondents must specify the maximum latency that will be exhibited between any two IP addresses within the network with 99 percent certainty, assuming the total IP traffic demand on the network does not exceed 90 percent of the maximum available bandwidth.

ETCOG will expect the total latency across the network, from any end-point to any end-point, not to exceed 50 milliseconds.

9.1.3 Packet Loss

Respondents must specify the maximum packet loss across the network. This specification must include any loss characteristics associated with links provisioned by the Respondent across another service provider's network and/or any applicable wireless links that comprise the proposed IP network.

ETCOG will expect the maximum end-to-end packet loss not to exceed 0.1 percent assuming the total IP traffic demand on the network does not exceed 90 percent of maximum bandwidth.

9.1.4 IP Deviation Variance (IPDV) (Jitter)

Vendors must specify the maximum IPDV from any end-point to any end-point IP through the network with 99% certainity. ETCOG will expect the maximum IPDV not to exceed five milliseconds for QoS protected packets, that is, for RTP packets, assuming the total IP traffic demand on the network does not exceed 90 percent of the maximum bandwidth.

9.1.5 QoS

The QoS system must insure that RTP stream packet loss and jitter remains below the specified values, even if lower-priority traffic demands significantly exceed the network bandwidth capability, and provided the RTP bandwidth demand remains below the 50 percent total bandwidth capacity provisioned over the path connecting the RTP endpoints.

9.1.6 Redundant Recovery Time

If redundancy is provided at the IP Layer (Layer-3), Respondents must describe the IP routing protocol and provide an estimated maximum re-route time for IP traffic should a failure occur at any point within the proposed redundant solution. The description should include the basis for the IP routing convergence time estimate.

If redundancy is provided at physical or media access layer, Respondents must explain the recovery scheme and time required for recovery at that layer.

ETCOG expects the redundant portions of the network to be able to automatically recover from hard failures, with IP traffic restored in under 5 seconds.

9.1.7 Network Availability

The network must be designed to "five nines" reliability. The actual realized in-service reliability for the core network and redundantly connected sites must exceed 99.99 percent in any month or the vendor must admit that service levels have been violated and be liable for remedy. This paragraph will not apply to a site where implementation of redundant facilities has been deferred.

9.1.8 Field Response Time and Mean-Time-to-Repair

If a network component fails at a site and requires service dispatch to that site, the Respondent must specify the maximum time required to position a service technician at the site. This time includes trouble ticket processing, dispatch, and travel. The Respondent must also list the maximum time from trouble ticket entry until a remote technician begins work on a reported problem.

The respondent must list the mean-time-to-repair, once repair is initiated, either in the field or remote repairs.

9.1.9 Service Level Agreement

Vendors must include a SLA for network performance that includes, at a minimum, all the items in section 9.1.

9.2 NETWORK MONITORING

The network must be monitored for proper operation and usage 7/24/365. The monitoring system must, at a minimum:

Perform a handshake, ping, SNMP status check, or other test with each managed network component at least every two minutes to insure that the monitored network component is in-service and is working as expected.

Detect circuit or facility failures through loss-of-signal, carrier, data, or high error rate alarms, or the use of test signals to verify circuit health. Circuit failure should not go undetected for more than two minutes by the terminating equipment.

The monitoring system should raise appropriate alarms within five minutes of any detected failure.

The system should log all alarms, all human interventions, and all in-service and out-of-service messages.

The monitoring system should record network traffic statistics at least every five minutes.

9.2.1 Reporting and NOC Operations

Vendors should supply a secure, online SLA/monitoring reporting system. Proposals should include a description of their reporting system. Reporting systems are expected to include real-time or near-real-time performance data captures in no greater than five minute averages.

The system should summarize network performance and traffic volume by hour, day, week, and month, or as specified by ETCOG. QoS reporting must present traffic by type and volume. The report should show traffic as a percent of network capacity.

Vendors should discuss how they will conduct and provide end of the month reviews, accounting for any degradation of service to include service failures.

Incidents must be tracked via tickets and the ticket contents, including resolution, must be made available to the participating entities via secure web site login or other agreed-upon means.

Upon request of ETCOG for a specified problem, the vendor must provide a root cause analysis coupled with steps to mitigate future occurrences of the problem within 30 days of the request.

9.3 REMEDIES

Vendors must specify financial remedies to ETCOG for each event in which service levels such as quality of service and network availability, are not maintained, on a monthly basis.

10. APPENDIX C – GLOSARY

http://www.infodiv.unimelb.edu.au/knowledgebase/

http://www.ietf.org/html.charters/ecrit-charter.html

NENA i3 Glossary

Newton's Telecom Dictionary Revision 22

Class of Service (CoS) - NENA Definition - A designation of the type of telephone service, e.g., residential, business, centrex, coin, PBX, wireless.

Class of Service (CoS) - The definition for packet switched networks used by VoIP and other packet technology. Networks, by design, typically provide best-effort delivery. Networks use CoS and quality of service (QoS) to manage traffic control. In an enterprise the different types of data that will transverse the network have different priorities. In an enterprise network, CoS differentiates high-priority traffic from lower-priority traffic. Tags may be added to the packets to identify such classes, but they do not guarantee delivery as do QoS functions, which are implemented in the network devices.

CoS is a way of managing traffic in a network by grouping similar types of traffic (i.e., e-mail, streaming video, voice, large document file transfer) together and treating each type as a class with its own level of service priority. Unlike QoS traffic management, CoS technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." On the other hand, CoS technology is simpler to manage and more scalable as a network grows in structure and traffic volume. One can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.

As networks have been more complex, managing CoS at the router level has become very complex. MPLS provides the ability to provide finer-grain CoS capabilities at the network level through expanded tagging capabilities.

Emergency Services IP Network (ESInet) - An IP-based inter-network (network of networks).

Geographic Information System (GIS) - A computer software system that enables one to visualize geographic aspects of a body of data. It contains the ability to translate implicit geographic data (such as a street address) into an explicit map location. It has the ability to query and analyze data in order to receive the results in the form of a map. It also can be used to graphically display coordinates on a map, i.e., latitude/longitude from a wireless 9-1-1 call.

Internet Protocol (IP) - The method by which data is sent from one computer to another on the Internet or other networks. IP is the IP part of TCP/IP family of protocols describing software that tracks the internet addresses of nodes, routes outgoing messages, and recognizes incomplete messages. IP is used in gateways to connect networks to the OSI network level 3 and above.

Jitter - Packets arriving at a non consistent rate due to a type of distortion caused by the variation of a signal from its reference that can cause data transmission errors, particularly at high speeds.

In voice over IP (VoIP), jitter is the variation in the time between packets arriving, caused by network congestion, timing drift, or route changes.

Mean Opinion Score (MOS) - A measurement of the subjective quality of human speech, represented as a rating index. MOS is derived by taking the average of numerical scores given by juries to rate quality and using it as a quantitative indicator of system performance. In multimedia (audio, voice telephony, or video) especially when codecs are used to compress the bandwidth requirement (for example, of a digitized voice connection from the standard 64 kilobit/second PCM modulation), the MOS provides a numerical indication of the perceived quality of received media after compression and/or transmission. The MOS is expressed as a single number in the range 1 to 5, where 1 is lowest perceived audio quality, and 5 is the highest perceived audio quality measurement.

The MOS is generated by averaging the results of a set of standard, subjective tests where a number of listeners rate the heard audio quality of test sentences read aloud by both male and female speakers over the communications medium being tested. A listener is required to give each sentence a rating using the following rating scheme:

Mean Opinion Score (MOS)

MOS	Quality	Impairment
5	Excellent	Imperceptible
4	Good	Perceptible but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

The MOS is the arithmetic mean of all the individual scores, and can range from 1 (worst) to 5 (best).

A similar process can be used to evaluate subjective video quality. A drawback of obtaining MOS estimations is that it may be more time-consuming and expensive as it requires hiring experts to make estimations. When a voice coding system is under development, or the developer has to test and compare a couple of audio systems, it's very important to have a possibility for a quick check.

Some suitable English-language phrases used for determining a MOS as suggested by ITU-T recommendation P.800 are:

- You will have to be very quiet.
- There was nothing to be seen.
- They worshipped wooden idols.
- I want a minute with the inspector.
- Did he need any money?

Mean Time Between Failure (MTBF) - MTBF is the arithmetic mean (average) time between failures of a system. The MTBF is typically part of a model that assumes the failed system is immediately repaired (zero elapsed time), as a part of a renewal process. This is in contrast to the mean time to failure (MTTF), which measures average time between failure with the modeling assumption that the failed system is not repaired.

Mean Time to Repair (MTTR) Rating - Basic measure of the maintainability of repairable items, it represents the arithmetic mean (average) time required to repair a failed component or device.

Multi-Protocol Label Switching (MPLS) - A mechanism that allows network administrators to perform a measure of traffic engineering within their networks.

MPLS is a data packet forwarding technology with improved forwarding speed of routers by using labels to make data forwarding decisions. When the data enters the first MPLS router, header analysis is done just once and a label is attached to the data packet. Subsequent routers forwards the packet by just inspecting the label and so it decreases the forwarding overhead on the subsequent core routers. IP packets have a field in their header that contains the address to which the packet is to be routed. Traditional routed networks process this information at every router in a packet's path through the network. This is not so in MPLS, where a label acts as a shorthand representation of an IP packet's header and carries the information that determines which path a packet should take. Nodes in the core MPLS network need not examine the packets header to perform next routing tasks.

National Emergency Number Association (NENA) - The National Emergency Number Association is a not for-profit corporation established in 1982 to further the goal of “One Nation-One Number.” NENA is a networking source and promotes research, planning, and training. NENA strives to educate, set standards, and provide certification programs, legislative representation and technical assistance for implementing and managing 9-1-1 systems.

Network Management System (NMS) – The system responsible for managing a portion of the network. The NMS talks to network management agents, which reside in the managed nodes, via a network management protocol. The NMS is the entry that implements functions at the Network Management layer. It may also include Network Management layer functions. A Network Management System may manage one or more other Network Management Systems.

Network Operations Center (NOC) – NOC is one or more locations from which control is exercised over a computer, television broadcast, or telecommunications network.

Large organizations may operate more than one NOC, either to manage different networks or to provide geographic redundancy in the event of one site being unavailable or offline.

NOCs are responsible for monitoring the network for alarms or certain conditions that may require special attention to avoid impact on the network's performance. For example, in a telecommunications environment, NOCs are responsible for monitoring for power failures, communication line alarms (such as bit errors, framing errors, line coding errors, and circuits down) and other performance issues that may affect the network. NOCs analyze problems, perform troubleshooting, communicate with site technicians and other NOCs, and track problems through resolution. If necessary, NOCs escalate problems to the appropriate personnel. For severe conditions that are impossible to anticipate – such as a power failure or optical fiber cable cut – NOCs have procedures in place to immediately contact technicians to remedy the problem.

NOCs often escalate issues in a hierarchic manner, so if an issue is not resolved in a specific time frame, the next level is informed to speed up problem remediation. Many NOCs have multiple "tiers", which define how experienced/skilled a NOC technician is. A newly-hired NOC technician might be considered a "tier 1", whereas a technician that has been there for several years may be considered a "tier 3" or "tier 4". As such, some problems are escalated within a NOC before a site technician or other network engineer is contacted.

The term NOC is normally used when referring to telecommunications and data services providers, although a growing number of other organizations such as public utilities (e.g., SCADA) and private companies also have such centers, both to manage their internal networks and to provide monitoring services.

The location housing a NOC may also contain many or all of the primary servers and other equipment essential to running the network, although it is not uncommon for a single NOC to monitor and control a number of geographically dispersed sites.

NOC locations can often house Security Operation Centers (SOCs).

NRIC Best Practices - the NRIC is an acronym for Network Reliability and Interoperability Council. A NRIC Best Practice is a technique, method, process, activity, incentive, or reward that is believed to be more effective at delivering a particular outcome than any other technique, method, process, etc. The idea is that with proper processes, checks, and testing, a desired outcome can be delivered with fewer problems and unforeseen complications. Best practices can also be defined as the most efficient (least amount of effort) and effective (best results) way of accomplishing a task, based on repeatable procedures that have proven themselves over time for large numbers of people.

Original Equipment Manufacturer (OEM) - An OEM manufactures products or components which are purchased by a second company and retailed under the second company's brand name. It is a form of outsourcing.

This term once meant "original equipment manufacturer" or the company that created and assembled the components of a computer that could be part of a larger solution. However, for many end product providers most components are now commodities, so OEMs like Dell don't actually manufacture components. In the real economic model they are middle marketers, assembling components and selling complete computers to customers or vendors. But since few people assemble their own computers, the label is still used.

Protocol - A set of rules or conventions that govern the format and relative timing of data in a communications network. There are three basic types of protocols: character oriented, byte-oriented, and bit-oriented. The protocols for data communications cover such things as framing, error handling, transparency, and line control.

Quality of Service (QoS), - As related to data transmission a measurement of latency, packet loss and jitter.

QoS refers to a broad collection of networking technologies and techniques. The goal of QoS is to provide guarantees on the ability of a network to deliver predictable results. Elements of network performance within the scope of QoS often include availability (uptime), bandwidth (throughput), latency (delay), and error rate.

QoS involves prioritization of network traffic. QoS can be targeted at a network interface, toward a given server or router's performance, or in terms of specific applications. A network monitoring system must typically be deployed as part of QoS, to insure that networks are performing at the desired level.
QoS is especially important for the new generation of Internet applications such as VoIP, video-on-demand, and other consumer services. Some core networking technologies like Ethernet were not designed to support prioritized traffic or guaranteed performance levels, making it much more difficult to implement QoS solutions across the Internet.
Using the Internet's Resource Reservation Protocol (RSVP), packets passing through a gateway host can be expedited based on policy and reservation criteria arranged in advance. The Common Open Policy Service (COPS) is a relatively new protocol that allows router and layer 3 switches to get QoS policy information from the network policy server.

Service Level Agreements (SLAs) - A contract between a service provider and the end user, which stipulates and commits the service provider to a required level of service.

A SLA is a negotiated agreement between two parties where one is the customer and the other is the service provider. This can be a legally binding formal or informal 'contract'

The SLA records a common understanding about services, priorities, responsibilities, guarantees, and warranties. Each area of service scope should have the 'level of service' defined. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service such as billing. The 'level of service' can also be specified as 'target' and 'minimum', which allows customers to be informed of what to expect (the minimum), whilst providing a measurable (average) target value that shows the level of organization performance. In some contracts penalties may be agreed in the case of non compliance of the SLA (but see 'internal' customers below). It is important to note that the 'agreement' relates to the services the customer receives, and not how the service provider delivers that service. Typical SLAs include statements about:

- System/service availability
- Time to identify the cause of a customer related notification
- Time to repair a customer related malfunction
- Service provisioning times
- Quality of service targets

Service Providers (SP) - An entity providing one or more of the following 9-1-1 elements: network, CPE, or data base service.

A service provider is an entity that provides services to other entities. Often, this refers to a business that provides subscription or web service to other businesses or individuals. Examples of these services include:

- Internet access
- Mobile phone operator
- web application hosting

Session Initiation Protocol (SIP) - An Internet Engineering Task Force (IETF) defined protocol (RFC3261) that defines a method for establishing multimedia sessions over the Internet. Used as the call signaling protocol in VoIP, i2 and i3.

SIP is a signaling protocol, widely used for setting up and tearing down multimedia communication sessions such as voice and video calls over IP. Other feasible application examples include video conferencing, streaming multimedia distribution, instant messaging, presence information, and online games. The protocol can be used for creating, modifying, and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. The modification can involve changing addresses or ports, inviting more participants, adding or deleting media streams, etc.

The SIP protocol is a TCP/IP-based application layer protocol. Within the OSI model it is sometimes placed in the session layer. SIP is designed to be independent of the underlying transport layer; it can run on TCP, UDP, or SCTP. It is a text-based protocol, incorporating many elements of the Hypertext Transfer Protocol (HTTP) and the Simple Mail Transfer Protocol (SMTP)[3], allowing for easy inspection by administrators.

Short Message Service (SMS) - A service typically provided by mobile carriers that sends short (160 characters or fewer) messages to an endpoint. SMS is often fast, but is not real time.

SMS is a communication service standardized in the GSM mobile communication system, using standardized communications protocols allowing the interchange of short text messages between mobile telephone devices. SMS text messaging is the most widely used data application on the planet, with 2.4 billion active users, or 74 percent of all mobile phone subscribers

sending and receiving text messages on their phones. The SMS technology has facilitated the development and growth of text messaging. The connection between the phenomenon of text messaging and the underlying technology is so great that in parts of the world the term "SMS" is used as a synonym for a text message or the act of sending a text message, even when a different protocol is being used.

Most SMS messages are mobile-to-mobile text messages, though the standard supports other types of broadcast messaging as well.

Simple Network Management Protocol (SNMP) – A protocol defined by the IETF used for managing devices on an IP network.

SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the IETF. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

Security Operation Center (SOC) - A (SOC is a centralized unit in an organization that deals with security issues, on an organizational and technical level. An SOC within a building or facility is a central location from where staff supervises the site, using data-processing technology. A purpose of a SOC is to provide real-time detection of cyber-attacks and security intrusions.

Because both NOC and SOC operation have very high reliability and security requirements, a SOC will often be part of a NOC operation.

Virtual Private Network (VPN) - A VPN is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

A VPN has the look and feel of a private network to a user. But it's really part of the internet with heavy security – so no one on the internet can see what's going on in the VPN. A VPN is not a private network, but virtually so. VPN technology was originally developed for voice networking, but subsequently was developed for use in data networking, as well.

Voice over Internet Protocol, Voice over IP (VoIP) – Provides distinct packetized voice information in digital format using the Internet Protocol. The IP address assigned to the user's telephone number may be static or dynamic.

VoIP is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. Other terms frequently encountered and synonymous with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, and broadband phone.

Internet telephony refers to communications services-voice, facsimile, and/or voice-messaging applications-that are transported via the Internet, rather than the public switched telephone network (PSTN). The basic steps involved in originating an Internet telephone call are conversion of the analog voice signal to digital format and compression/translation of the signal into IP packets for transmission over the Internet; the process is reversed at the receiving end.

VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs which encode speech allowing transmission over an IP network as digital audio via an audio stream. Codec use is varied between different implementations of VoIP (and often a range of codecs are used.

Wide Area Network (WAN) – Network using common carrier-provided lines that covers an extended geographical area. WANs usually connect many Local Area Networks (LANs). The most commonly recognized WAN is the Internet.

11. ATTACHMENT D – CPE FUNCTIONAL REQUIREMENTS

Respondents proposing CPE equipment for Longview Police Department and/or Champion EMS must complete the functional requirements matrix for each proposed solution.

Please see Attachment D