The Commonwealth of Kentucky
NG9-1-1 State Plan

August 1, 2009

Prepared by

Kentucky Commercial Mobile Radio Service Board

Kentucky Office of the 9-1-1 Coordinator/CMRS Board
Kentucky Office of Homeland Security
Office of the Governor
200 Mero Street
Frankfort, KY 40601
Ph: (502) 564-3911
Fax: (502) 696-5295
www.cmrsboard.ky.gov

RCC CONSULTANTS, INC.

Public Safety Information Systems
2425 Millcreek Court
Tallahassee, Florida 32308-4375
Voice: (850) 224-4451 Fax: (850) 224-3059
www.rcc.com

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. EXECUTIVE SUMMARY

The Commonwealth of Kentucky and the Kentucky Office of Homeland Security through the Commercial Mobile Radio Service (CMRS) Board in conjunction with local government and communications providers of the Commonwealth have decided on a course of action to improve 9-1-1 emergency communications through the adoption of new technologies. The result of this collaboration will result in improved interoperability among the Public Safety Answering Points (PSAP) and quantum improvements to the delivery of emergency services.

Through deliberate and thoughtful research, the conclusion was reached to deploy an IP based network intended to receive, process, route and deliver all calls to 9-1-1 within a State of Kentucky Managed Network. Commonly referred to as Next Generation 9-1-1 this network will benefit all the stakeholders including citizens and visitors to the Commonwealth, PSAPs, first responders and legislative and decision makers.

It has been recognized that the current delivery methods of 9-1-1 is hindered by outdated technologies and networking. Current methods of adopting emerging technologies are hindered, if not blocked, by the analog environment traditional 9-1-1 systems employ. As is common within the United States the evolution of 9-1-1 is based upon local government's ability to provide this service. The unmistakable result is a collection of independent and stand-alone deployments with little if any ability to utilize available resources to the benefit of emergency services. Migration from today's legacy analog systems to a privately managed IP network will result in the mitigation of these issues to the benefit of all.

The deployment of this network will provide a uniform method of call delivery without regard to PSAP size or capabilities and offer the service provider a streamlined method of delivering calls to the emergency service providers of the Commonwealth. Elimination of the artificial barriers to call delivery attendant to legacy systems greatly improve the quality of service and bring a uniform method to calls for service.

This cost-effective solution will offer a clear path to the future within the Commonwealth. With a uniform method of call delivery, receipt and handling, each participating entity will be an equal within the first responder community of Kentucky. As such, all 9-1-1 services within the Commonwealth will reach a higher level of service; at a lower recurring cost for local governments, citizens and service providers thru the Board's actions of managing cost and service delivery via the implementation of this Plan.

2. INTRODUCTION

The Commonwealth of Kentucky and the Kentucky Office of Homeland Security, through the Commercial Mobile Radio Service (CMRS) Board (hereinafter referred to as "Board"), has embarked upon the effort required to transition to an Emergency Services IP Enabled Network (ESInet). Accordingly, a deployment strategy and plan is required. When requesting funds from outside the Commonwealth, this plan will be used to identify the processes and predicted outcomes to those not directly involved in this process.

This document represents the Commonwealth's NG9-1-1 plan for the statewide deployment of an ESInet. The NG9-1-1 Standards Report, which is referenced herein, discusses in more details the technical aspects of NG9-1-1. The NG9-1-1 Standards Report is included in this NG9-1-1 State Plan in Appendix B.

This network is to be provided by a System Service Provider (SSP) and will not be privately held by the Commonwealth. The acquisition of services will require a Request for Proposal (RFP). This RFP will act to qualify vendors regarding their ability to install, maintain, and operate an ESInet in accordance with this plan and have the qualities of being capable of continuing operation into the future. Thus, the following outline for deployment is envisioned:

1. Identification of funding.
2. Identification of participating Commonwealth entities.
3. Preparation, distribution, and analysis of the RFP responses.
4. Award to successful SSP.
5. Negotiations for performance terms.
6. Initial installation and testing.
7. Initial PSAP connection and testing.
8. Commonwealth approval for "go live".
9. Continuation of deployment.
10. Periodic review of current standards and best practice.

It is the clear intent of the Commonwealth and the Board to create an IP-based network intended to transport and deliver emergency calls regardless of the source. The Board is clearly committed to this effort and will work to ensure the tenets of this plan are realized.

3. NG9-1-1 OVERVIEW

Throughout the last decade, communications have been advancing at a fast pace and it is only logical that 9-1-1 services evolve to meet the current technological advancements. In an effort to meet these requirements, NG9-1-1 has been developed. Standards are at the very heart of NG9-1-1 communications, they serve to assure the ability to communicate across distance in a reliable and predictable manner.

As with any other standard, NG9-1-1 is still evolving but enough of the baseline network is available as a standard to assure success. Much of the remaining standards work involves the definition of new technologies and, in fact, technologies that are "over the horizon". This report reflects the current available standards and should serve as a foundation for moving forward with NG9-1-1.

3.1 NG9-1-1 Capabilities

NG9-1-1 enables a wealth of enhanced emergency (9-1-1) request processing and response capabilities including:

1. Enables present and future handset technology such as the delivery of text messages, video, and images to Public Safety Answering Points (PSAPs) and emergency responders.

2. Support for the delivery of telematics device information (automatically detected automobile accidents, health alarm monitors, and other emergency detection devices) directly to a PSAP without having to go through an intermediary call center.

3. Enhance support for VoIP emergency calls.

4. Pre-validated location information delivered with the emergency request rather than after the emergency request is delivered to a PSAP.

5. Robust emergency request routing that supports the automatic re-routing of emergency requests (9-1-1 calls) if the destination PSAP is inoperable or busy.

6. Adoption of policy, rules, and procedures that will automatically route an emergency request to the appropriate PSAP.

7. Enables access to supplemental incident information available on a variety of emergency databases, law enforcement/crime databases, medical databases, records management, hospital, court, jail management, and other relevant systems that interface each other through the NG9-1-1 network.

8. Speeding up the delivery of emergency requests to the appropriate PSAP.

9. Cost and operational efficiencies gained through the use of standardized interfaces

among disparate systems and databases.

10. Rapid support for emerging technologies in emergency request processing and response.

These enhanced capabilities are available under NG9-1-1 while support for existing 9-1-1 capabilities such as enhanced 9-1-1, phase I wireless, and phase II wireless are maintained.

4. RELATIONSHIPS

4.1 CMRS Board and PSAP

The purpose of this section is to provide a blueprint of the relationships between the governmental entities that deliver 9-1-1 services within the Commonwealth. Common to this effort across the United States is the establishment of a form of governance that assumes responsibility for a variety of functions required to successfully deploy NG9-1-1 applications in a uniform, unbiased fashion. Within the Commonwealth, this oversight takes the form of the Kentucky Office of the 9-1-1 Coordinator/Commercial Mobile Radio Service (CMRS) Board. In order to best serve the citizens of the Commonwealth, the Board has undertaken strategic steps toward forming a body that, through consensus, offers services both real and through guidance in the advancement of NG9-1-1. Strategies include:

1. Designation of a statewide 9-1-1 coordinator who has authority and oversight of resources to effectively implement NG9-1-1.

2. Establish a baseline to determine where resources are needed to complete the NG9-1-1 system.

3. Identify opportunities to efficiently fund implementation.

4. Provide education and outreach to PSAPs to assist them with implementation.

The Commonwealth is in the position to mitigate current barriers for NG9-1-1 by the recent appointment of a 9-1-1 coordinator and the attendant responsibilities to guide the Commonwealth toward a successful implementation of a NG9-1-1 deployment.

The most essential function of the Board and the 9-1-1 coordinator will be the design, award and ongoing oversight of the basic ESInet[1]. The acquisition of the ESInet should be a process of an open Request for Proposal (RFP) to provide both connectivity and application software. Included in the RFP will be the description of what is expected regarding Quality of Service (QoS), sizing, and traffic reporting. Contract service terms, including response escalation for system outages, will also be clearly specified in the RFP. The Board, through the 9-1-1 coordinator, will act as the facilitator regarding the installation at each PSAP, or group of PSAPs, with the required network components in a manner consistent with the Commonwealth's plan of deployment. Further, the 9-1-1 coordinator will support the PSAPs by answering NG9-1-1/ESInet implementation questions that arise.

Funding for this network is to be coordinated by the Board for the benefit of the PSAPs. By coordinating the collection and distribution of funds for the network, the Board will provide a single point of focus for network and application processes. Following the award of the ESInet contract, and using the deployment strategies of this plan, payment of non-recurring and

[1] For purposes of this plan the ESInet includes the network and its component parts and applications.

recurring expense of the ESInet will be administered at the Board level.

As NG9-1-1 continues to evolve, the Board may be required to create certain Administrative Rules regarding the deployment as allowed by statute[2] and to assure an effective and efficient use of this resource for the benefit of the Commonwealth.

The Board, through the 9-1-1 coordinator, will create periodic reports regarding the status of the deployment and share such reports with the PSAPs through an appropriate venue. Regular reporting will keep lines of communication open and foster improvements to the project by allowing interaction among the various stakeholders.

4.2 Inter-PSAP

Due to its flexible nature, the ESInet opens new avenues to individual PSAPs regarding all aspects of call routing and call handling. No longer limited by barriers imposed by analog components such as selective routers, the PSAP will need to consider options when migrating to an IP-based environment. In considering operational parameters, most details are simple while some are unique and offer qualified improvements to the manner in which calls are handled today. Depending on how a PSAP may wish to leverage this powerful network, certain PSAP-to-PSAP agreements may be required.

A sampling of issues to consider includes such topics as:

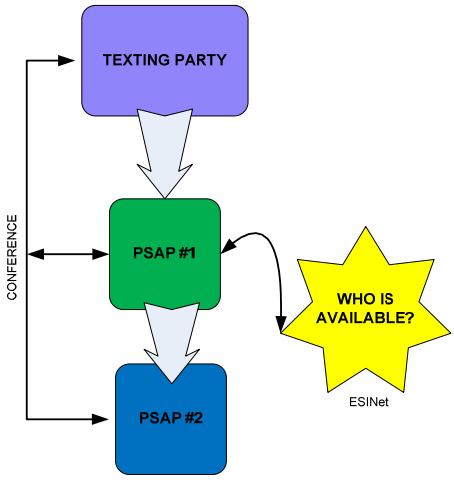
1. Providing the ability to establish a call path to/between multiple communication devices.
2. Providing the capability to establish voice conferencing.
3. Providing the capability to establish video conferencing.
4. Providing the capability to establish interactive text conferencing.
5. Providing an indicator that additional data is available.
6. The system shall support the allocation of resources supporting multiple staffing levels, which can be based on busy-hour(s), busy-day(s), busy-season(s), and special event data (for example, call taker training, language, media type proficiency).
7. The system shall route calls based on the associated call treatment process by the PSAP's business rules.
8. The system shall be capable of providing alternate call treatment for potentially redundant calls within a defined geographic area.

[2] Kentucky Revised Statutes (KRS) 65.7629 *Powers and duties of the Board.*

9. Providing alternate call routing capability, including distribution to an alternate location, a pre-recorded message that includes the ability to transfer to another location, a fast-busy signal, and other predefined call treatment or combination of treatments.

Planning on how to form relationships among the Commonwealth's PSAPs will be an activity best taken on a local basis. Local rules, policies, and procedures should not be expected to be directed at the Board level. However, the Board can play an essential role in fostering the kind of PSAP-to-PSAP conversations that will take best advantage of the network being deployed. This said, Figure 1 depicts how a PSAP can find a call-taker, virtually anywhere on the network that is listed as an expert at "texting" and is available to take a call:

Figure 1 Texting Assistance Example



In this example, one of several scenarios may play out based on inter-PSAP agreements. In this case PSAP #1 needs assistance with a texting caller. The ESInet is polled to determine an available call taker who is listed as an expert at texting. PSAP #2 is identified and a conference "call" is established. Call history is advanced to PSAP #2 who takes control of the messaging and interprets for PSAP #1, who is responsible for call disposition.

This admittedly, simplified example shows the power of the network and the associated applications, business rules in this case, that may allow improved call handling and better uses of available resources. It also points to the requirement that PSAPs must interact in a positive manner to bring this type of solution to bear. Expectations must be clearly identified in order to allow all parties to make informed decisions.

5. DEPLOYMENT

5.1 Summary of Conceptual Network Design

The conceptual design for the Commonwealth ESInet is one that will meet the Commonwealth's requirements initially and be adaptable and scalable to the changing types of communications that NG9-1-1 is intended to support. At the core of the proposed network is a Multi-Label Protocol Switching (MPLS) backbone as provided by an MPLS carrier.

The proposed MPLS network will support traditional voice 9-1-1 traffic as well as video and data traffic. Voice, data, and video traffic, regardless of its source, are transmitted on the network as data packets. In order to maintain voice quality, voice traffic must be prioritized. Quality of Service (QoS) features must be implemented in the proposed network for this purpose. Specifically, the National Emergency Number Association (NENA) recommends that the Differentiated Services (DiffServ) QoS protocol be implemented. This will be a requirement that the selected carrier will implement and manage in the network.

At a minimum, two geographically diverse data centers are required, each with the capacity to handle the entire call volume, in case one of the data centers is off line for any reason. A three-center configuration is best practice, since it maintains redundancy even if one data center is unavailable, whether due to an emergency, preventive maintenance, hardware/software upgrade, or any other reason.

Each data center shall have full capability of supporting all the 9-1-1 traffic originating in the Commonwealth. Full capability is defined as including Border Control Function, Routing, and rules-based servers. It is imperative that all calls delivered to the ESInet can appear at each center with call management handled as "overhead" between the load sharing capabilities of these centers.

The Board will obtain MPLS services as a managed/routed solution. This approach requires the MPLS carrier to implement routing protocols based on policies and direction decided by the Board. An example of this would be through the establishment of "load sharing" among the data centers. As one center may concentrate on a geographical area of the Commonwealth, the remaining centers are entirely capable of routing to any PSAP. Thus, the Board can concentrate on how and where it wants traffic routed, while the service provider is responsible for the technical elements of configuring and managing the configuration of the network and data center devices. In this case, for example, the Board will establish routing policies that require the carrier to automatically sense failure at a center or network route and re-route traffic through an alternate data center and data path if the geographically responsible data center fails; and the carrier will configure the routers to respond accordingly.

The Board will determine whether it wants a primary data center, and one or more backup data centers; or whether it wants to load balance all traffic among all data centers. Load balancing is more complex, but is feasible using the proper routing protocols. Routing all traffic to a primary data center, with the other data centers serving as hot standby is simpler to manage from a

routing perspective but lacks the robust fail-over features of Open Shortest Path First (OSPF) configuration.

The design envisions that all 9-1-1 calls from all sources – landline, cellular, and Internet – will be delivered to, and aggregated by the selected MPLS carrier, transported as data packets, and routed to the data centers through the MPLS network. Routers at the carrier's location will route calls to the data centers based on rules developed by the Board (i.e., load balance among the data centers or select a primary data center to handle all traffic, and have the other data centers act in a backup role in the event of a failure of the primary data center or network link).

Calculations have determined that the network links from the data centers to the ESInet should be sized at 200 Mbps[3] initially. This bandwidth meets the P.01 grade of service, based on existing call volumes. These links will support the following traffic types:

- Incoming 9-1-1 calls from the carriers.
- Outgoing 9-1-1 calls to the PSAPs.
- Database synchronization functions.

Typically, database reconciliation will be a scheduled activity to occur during periods with low 9-1-1 call volumes so as not to interfere with emergency calls. Furthermore, database reconciliation functions will be assigned a lower priority within the QoS structure, ensuring that 9-1-1 calls are treated as the highest priority. The Service Level Agreement (SLA) between the Board and the MPLS carrier shall include a requirement for the provider to monitor traffic loads and upgrade (or downgrade) the capacity of the network links in response to changing call volumes and types.

The Board will identify key PSAPs that handle high call volumes, and work with the selected carrier on a case-by-case basis to investigate diverse paths. Other PSAPs can meet redundancy requirements via partnerships and business rule routing during incidents that compromise service call receipt.

In the Network Sizing section of the NG9-1-1 Standards Report, calculations have been provided estimating the size of the links from the ESInet into each PSAP. In most cases, a single T1 will support the existing call volumes. In a small number of cases, multiple T1s are required.

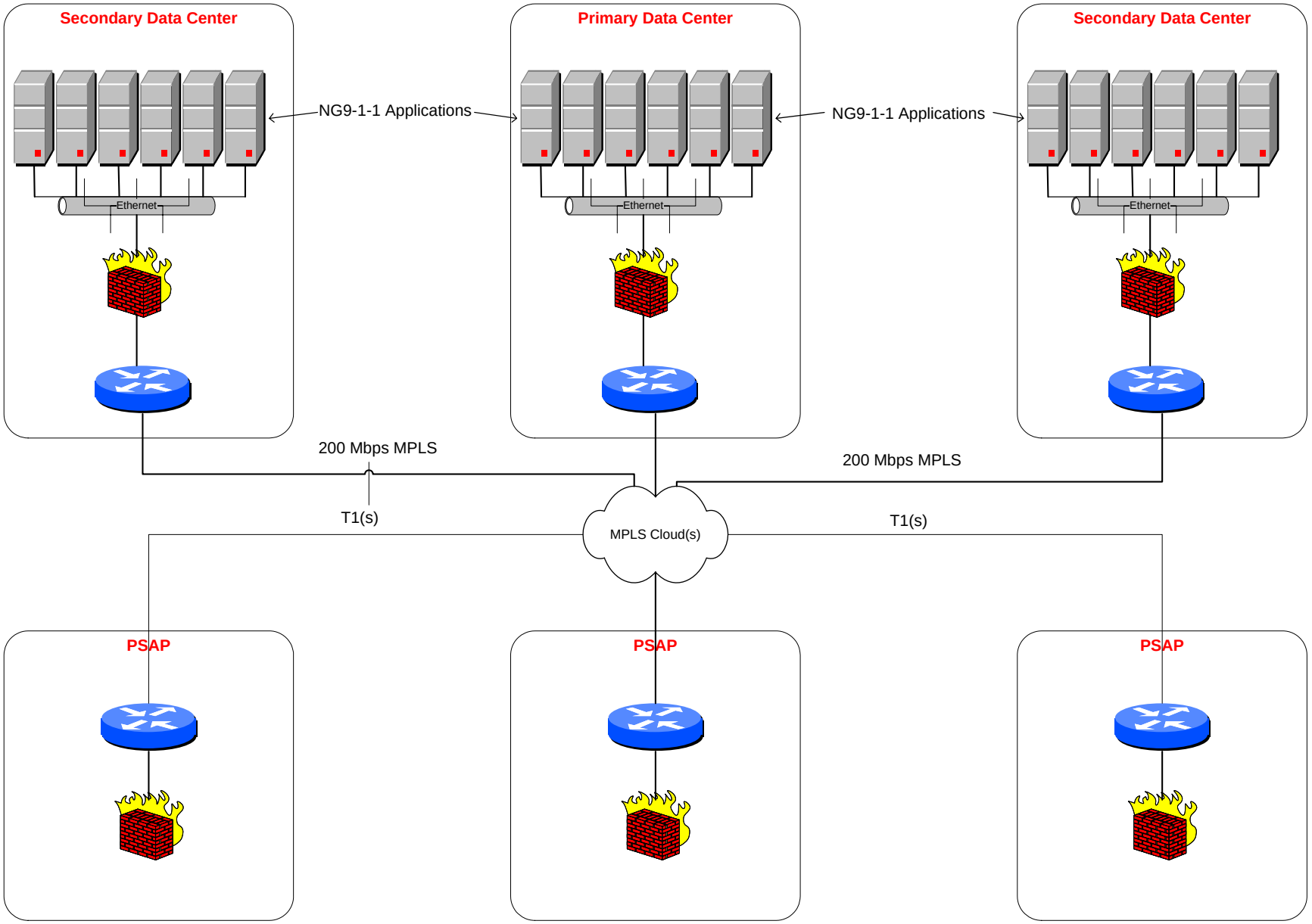
Note that the sizing estimates are intended to support the existing voice-only traffic into the PSAPs. There is no empirical data upon which to base an estimate for future non-voice 9-1-1 traffic. The awarded network provider can quickly upgrade links or add bandwidth to support

[3] The 200 Mbps Link will support both traffic routed in to the ESInet from the service providers and the traffic routed through the ESInet to the PSAPs.

additional traffic when it occurs.

In awarding the ESInet, the Board will require estimates from the bidders regarding recurring and non-recurring expenses. The Board will be required to identify funding sources for these activities to ensure the long-term provision of this service.

Figure 2 Conceptual Network Diagram


Secondary Data Center
Primary Data Center
Secondary Data Center
NG9-1-1 Applications
NG9-1-1 Applications
Ethernet
Ethernet
Ethernet
200 Mbps MPLS
200 Mbps MPLS
T1(s)
T1(s)
MPLS Cloud(s)
PSAP
PSAP
PSAP

5.2 Implementation Phasing Plan

5.2.1 Data Centers and Applications

Redundant and robust servers must be strategically placed[4] within the ESInet to host the ESInet/NG9-1-1 applications. The servers may be located at a service provider's data center, or at an agency site, depending on the final network design, business model, and service level agreements. As with the ESInet, each server and application must be implemented with an operational continuity availability of at least 99.999% at the component level.

A primary design consideration is the location and quantity of data centers that will house the primary NG9-1-1 applications. The plan provides for three geographically diverse data centers. Each must have the capacity to handle the entire call volume, in case one of the data centers is off line for any reason, which maintains redundancy even if one data center is unavailable, whether due to an emergency, preventive maintenance, hardware/software upgrade, or any other reason.

The data centers are the nucleus of the ESInet, and integral for its successful operation. Therefore, one of the first steps of the implementation plan will be the deployment of all the hardware and software at the identified three data centers, including the servers and the NG9-1-1 applications. All the data centers should be configured, online, and tested before the ESInet processes any "live" calls. Section 5.3 goes into the details of the acceptance test plan.

5.2.1.1 ESInet/NG9-1-1 Applications

The NG9-1-1 applications and the appliances they operate on enable the NG9-1-1 capabilities and normally lie in the path of all call signaling and media. Like the network, the applications must be efficient and highly reliable, meeting the same level of reliability, in order to support emergency operations without adding any significant delays to emergency request processing. The major applications that are resident on the ESInet include at least the following components:

1. Border Control Function (BCF).
2. Emergency Call Routing Function (ECRF).
3. The Location to Service Translation (Lost) protocol.
4. Emergency Service Routing Proxy (ESRP).
5. Location Validation Function (LVF).
6. Legacy Network Gateways.

[4] Strategic placement implies geographic separation.

7. Business Rules.

Details regarding the above components are included in the NG9-1-1 Standards Report, Appendix B.

5.2.2 Initial Deployment (Proof of Concept)

The recommended methodology to deploy the NG9-1-1 system is a phased installation. Phasing the installation allows several checkpoints during the implementation to confirm that all services are functioning properly and per specification, and to identify and correct any issues that arise. In general, the proposed approach starts with a small "proof of concept" installation, and then proceeds to expand the system and introduce the necessary layers of complexity until the installation is complete. At each milestone along the way, the system and network are tested to demonstrate compliance with the Board's expectations for functionality and service levels.

A critical first task in deploying the system is the selection of sites to serve as data centers. Three data centers offers a level of service that will maintain redundant operations even when one of the sites is taken down for routine or preventive maintenance, or due to component or network failure. In 2005, the Telecommunications Industry Association (TIA) released TIA-942 Telecommunications Infrastructure Standards for Data Centers. TIA-942 covers the following:

1. Site space and layout.

2. Cabling infrastructure.

3. Tiered reliability.

4. Environmental considerations.

TIA-942 describes detailed architectural, security, electrical, mechanical, and telecommunications recommendations. The Board should adhere to TIA-942 as it selects its data center sites, and use the standards to evaluate and compare alternative locations.

Another factor involves selecting data center sites where the location of the center is, in relation to the network service provider's network. Sites that offer diverse entrance points and geographically diverse paths to the service provider's location are preferable.

Once the Board has selected the sites and deemed them ready for installation of the NG9-1-1 and ESInet services, the first data center should be deployed. All applications should be implemented, tested, and proven functional per the specifications prior to cutting over live calls to the ESInet. The remaining data centers should be deployed and receive these same tests once the primary center is completed and tested.

Concurrently with the data center implementations, the network links from the data centers to the MPLS network will then be ordered, installed, and thoroughly tested. Once the network links

are in place, critical network and application functions including call routing into the network, re-routing of calls due to network or component failures, load balancing, throughput, QoS, security services and database backups across the network can be tested.

The next element of the deployment is the selection of PSAPs to participate in the proof of concept. A small number of PSAPs shall be selected using pre-identified criteria including the following:

1. Relatively small call volumes.

2. Adjacent PSAPs with existing relationships in place for 9-1-1 call coverage during outages or major incidents.

3. Directly served by the selected network service provider.

4. Knowledgeable of and active in the NG9-1-1 project planning.

With the network links to the data centers and initial PSAPs now in place, call routing and re-routing functions can be tested using simulated traffic. Once all routing, re-routing, QoS, and network security functions are demonstrated to be operating per the specification, a cutover of the initial PSAPs can be planned and scheduled. A clear and detailed acceptance testing plan will be developed by the Board, the network service provider, and the NG9-1-1 applications provider to demonstrate compliance with the specifications.

5.2.3 Roll Out of Remaining PSAPs

The planning process for the roll out of the remaining PSAPs should occur concurrently with the roll out of the initial PSAPs. A phased approach introduces increasing levels of complexity as the implementation progresses. Complexity levels include:

1. PSAPs that carry higher call volumes.

2. PSAPs with higher numbers of call takers.

3. PSAPs served by carriers other than the primary network service provider, rolled out by carrier (i.e., all of carrier X's PSAPs rolled out as a single cutover).

Each step is designed to add PSAPs, call traffic, and routing and re-routing complexity to the network. Each step is intended to include careful monitoring of the impact to the new PSAPs to network throughput, and testing and re-testing of functions demonstrated during prior phases to confirm that no degradation of service occurs as new PSAPs are added.

5.3 Testing and Acceptance Plans

The Board will negotiate a final Acceptance Test Plan (ATP) during the contract negotiations with the successful provider. At a minimum, the ATP shall include the following:

1. Functional acceptance test.

2. Throughput acceptance test.

3. Reliability acceptance test.

The ATP will be conducted before a PSAP (or group of PSAPs) is cutover. All the applications and appliances installed are considered mission critical, and it is crucial for the safety of the citizens, within the Commonwealth, that they are fully functional and reliable before they are put into productive use.

5.3.1 Functional Acceptance Test

Part of the contract negotiation process with the service providers and/or vendors for a turnkey solution includes the detailed configuration design to determine exact functionality and the degree of integration between the different components of the system including the data centers and PSAPs. The functional acceptance test will be conducted to verify that the systems installed provide the expected functional capabilities in accordance with the detailed configuration design criteria. The service provider will be expected to demonstrate to the Board that each function and option operates according to the detailed configuration design documentation that will be created during contract negotiations.

It is essential to ensure that the implemented system is operating according to the functional requirements identified before the Board moves forward to the second phase of the acceptance test plan.

5.3.2 Throughput Acceptance Test

The service provider should conduct and pass system throughput performance tests for each PSAP, data center, and for the complete system as a whole. These tests verify that the installed applications and equipment meet the expected throughput capability and provide the expected operational speed and growth potential. The amount of throughput to be tested will be based on the peak number of transactions experienced by the PSAPs, combined with the selected service provider's claim for system throughput capability. The service provider will be required to execute and provide a standard benchmark test based on peak load characteristics with a transaction rate corresponding to the system loading information.

5.3.3 Reliability Acceptance Test

The Board will test the installed systems to ensure that they meet the service provider's claims for reliability or the Board’s own minimum standards for reliability, whichever is greater. The reliability test will last a minimum of 90 days and be conducted against three standards, one for each of the following:

1. Hardware and related equipment.

2. Software.

3. Network.

The Board will create detailed standards for each one of the three components identified above. As identified through this document and through the NG9-1-1 Standards Report the hardware, software, and network (individually as components) will operate at a 99.999% reliability and availability standard. These standards will flow through to the reliability test plan due to the critical nature of the systems implemented.

The acceptance test for the network should demonstrate that the network meets or exceeds requirements that will be stated in the SLA regarding:

1. Latency.
2. Jitter.
3. Throughput.
4. Routing and automatic re-routing.
5. Network security functions.
6. Load balancing (if implemented).

5.4 Deployment Schedule

The Board has included the following deployment schedule based on the grant program schedule. The Board has allocated the resources and funds to fully engage in this effort as soon as the project is kicked off and will be ready to augment the resources as needed to meet the time restraints identified in the grant application.

Table 1 Project Deployment Schedule

Milestone	Date Completed
Project Kickoff	October 1, 2009
Prepare RFP for ESInet Procurement	December 1, 2009
Receive Vendor Proposal	February 1,2010
Evaluate Vendor Proposal	March 1, 2010
Select a Vendor	April 15, 2010
Contract Negotiation	June 1, 2010
Vendor Awards	June 1, 2010
Install, Configure and Test Data Centers	September 30, 2010
Deploy and Test Proof of Concept PSAPs	October 31, 2010
Deploy and Test Phase 2 PSAPs	June 30, 2011
Deploy and Test Phase 3 PSAPs	October 31, 2011
Deploy and Test Phase 4 PSAPs	February 28, 2012
Deploy and Test Phase 5 PSAPs	June 30, 2012
Final Performance Period (90 days)	September 30, 2012

6. PSAP SYSTEM REQUIREMENTS

Upon implementation of the ESInet, PSAPs will have a tangible incentive to upgrade existing PSAP equipment, and take full advantage of the features of NG9-1-1. If there are any limitations for the PSAPs to upgrade their systems, they can still access the ESInet via legacy network gateways that will allow them to receive E9-1-1 calls over the ESInet using their existing equipment. Other requirements for system upgrade or replacement include hardware interfaces, operational considerations (e.g. training), and supported PSAP software applications.

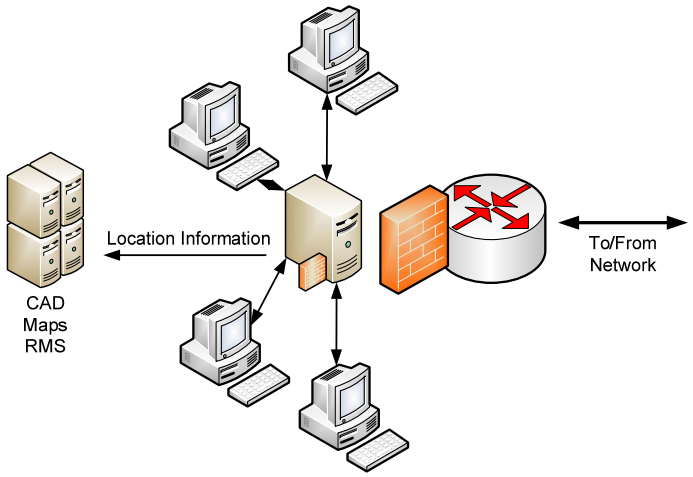


Figure 3 Typical PSAP Configuration

6.1 PSAP System Requirements to support NG9-1-1

6.1.1 NG9-1-1 Network Connection

IP-capable PSAPs will connect directly to the ESInet via a local firewall and router. Legacy PSAPs (non-IP-capable) will connect to the network via an external gateway that provides signal conversion to/from the NG9-1-1 system.

As with the current physical connection to the 9-1-1 phone trunks, the connection to the NG9-1-1 Network should be reliable and redundant. Service level agreements will be executed to guarantee the public safety-level of service in “last mile” connections to the NG9-1-1 network. PSAPs can obtain physical circuit redundancy by duplicating PSAP entrance facilities. This would mitigate network disconnections due to physical damage to the Network Entrance (i.e., damage to entrance cable caused by excavation equipment).

6.1.2 Call Handling Appliances/GIS

Call Handling Appliances within the PSAP will connect to the GIS/mapping system. Typically, the Customer Premise Equipment (CPE) will transfer caller location data to the mapping system to provide graphic presentation of the caller’s location.

6.1.3 Call Handling Appliances/Public Safety Dispatch Systems

Data from the 9-1-1 calls will continue to be captured by public safety dispatch systems within the PSAP. This will require connection between Call Handling Appliances and the following dispatch system components (at a minimum).

1. Computer Aided Dispatch.
2. Records Management System.
3. Logging system.

Standards for interfaces with these systems are forthcoming from communications standards development bodies (i.e., APCO, ITU, NENA, TIA, etc.).

These systems will potentially require modification to support the capture of additional data transmitted with new 9-1-1 calls (i.e., text, pictures, and video).

6.1.3.1 Computer Aided Dispatch (CAD) System

New data will be available for the CAD system to capture and process. For example, at PSAPs where the CAD system is used to display caller location, the CAD GIS will have to receive and process LON/LAT data instead of a local x,y coordinate system.

The NG9-1-1 system will also allow call takers to transmit CAD data to other PSAPs to support call transfers and mutual aid responses.

PSAP management personnel could upgrade CAD systems to support these operations and/or require these CAD system functions in new system procurements.

6.1.3.2 Records Management System (RMS)

The ESInet will facilitate the sharing of RMS data among public safety agencies Statewide (and eventually beyond). This will require a digital connection, an “outbound” query-access interface to allow RMS data to be shared on the ESInet, and an “inbound” query-access interface to allow users to query the local RMS.

Agency command personnel could upgrade RMS systems to support these operations and/or require these RMS interfaces in new system procurements.

6.1.3.3 Logging System

Future logging systems will be able to capture more than just voice recordings. Text, video, and telematic “calls” received at the PSAP could be recorded, time stamped, and available for replay. Captured call information should also be transferrable to other agencies for call transfers and mutual aid responses, via the ESInet.

6.2 Future Enhancements

6.2.1 Approval Process Future PSAP Applications to Access the ESInet

The Board will develop minimum specifications for applications that will be connected to the ESInet. These specifications will be "generic" so that they could be included into almost any procurement document (i.e., RFP, ITB, etc.) for an application that would potentially be connected to the ESInet. The Board could also review/approve application design submittals for compliance with the standards.

At a minimum, the Board's ESInet Applications Approval Process specifications should address:

1. Connection protocols.
2. Internet Protocol specifications.
3. Security standards (i.e., firewall requirements, approved software, user access permissions, username/password standards, etc.).
4. Training and certification requirements for users and system administrators.
5. Vendor certification.

7. GIS STANDARDS REQUIREMENTS

As stated in the NG9-1-1 Standards Report (Attachment 'A'), "In NG9-1-1, GIS becomes one of the central data stores for the delivery of emergency services. All call location and routing functions will be based on geospatial datasets that drive the major components of NG9-1-1, including the Location Information Server (LIS), Validation Database (VDB), Emergency Service Zone Routing Database (ERDB), Emergency Call Routing Function (ECRF), and Emergency Call Routing Proxy (ECRP)." Because the NG9-1-1 delivery system is using GIS to route the calls, the GIS database takes on a completely new level of importance. This significant change includes the requirement that the database become and continues to be extremely accurate. There must be consistency and preciseness within the GIS database itself, between its various layers, and as compared to Master Street Address Guide (MSAG) and the Automated Location Information (ALI). Another requirement in NG9-1-1 is that the GIS must have a more regional area of coverage as opposed to the current standard model of only a county. The need for both state and national 9-1-1 GIS databases for call validation and routing is imminent.

The Board has communicated these requirements to the individual PSAPs, coordinating their efforts to upgrade and enhance their street centerlines and jurisdictional boundary files and has successfully merged them into seamless, statewide datasets. The PSAP certification process and audits implemented by the Board has provided a solid foundation to support the PSAPs in their synchronization of their GIS databases and their MSAG and ALI. This process will run concurrently with the definition, funding, and implementation of the ESInet and, as with the ESInet, legacy systems and datasets will continue to function until final cutover to NG9-1-1.

The NG9-1-1 Standards Report details the issues and mechanics of bringing current GIS datasets to the standards that have been and continue to be developed and published by the National Emergency Number Association (NENA). The Board will continue the implementation of the enhanced GIS through the following actions:

1. Complete the certification of the remaining PSAPs based on current standards.

2. Revise PSAP Audit and Survey process and materials to increase level of detailed information being provided.

3. Use tools and the communications network to introduce to PSAPs the advantages of data scrubbing via the comparison of GIS data, MSAG, and ALI databases.

4. Further promote and develop the relationships between PSAPs and their respective Area Development Districts (ADD) to support this effort.

5. Fully access and engage all support and assistance available through NENA.

While these steps are not all-inclusive and will need to be further detailed as the Board begins to implement their Plan, they will serve as a general blueprint for proceeding with this critically important task of developing a highly accurate and consistent GIS database.

8. TRAINING REQUIREMENTS

The implementation of NG9-1-1 will have a tremendous impact on 9-1-1 operations. All 9-1-1 system users will require training on the new system functionality. These "users" include: PSAP calltakers/dispatchers, third-party service providers, public safety responders, as well as the general public.

8.1.1 PSAP Call Takers/Dispatchers Training

A dramatic increase in call/incident information will come with the implementation of NG9-1-1. Public Safety Call Takers will be receiving emergency information in the form of voice calls, TTY/TDD calls, cell phone calls, VoIP calls as well as text messages, video, and still pictures.

To prepare for the efficient processing of these new call types, call takers will require additional training (and screening). The following new processes and procedures should be addressed:

1. Process text messages. Call takers will be required to receive and respond to text messages received from the public. Citizens who are proficient in "texting" use an abbreviated language that reduces keystrokes (i.e., ttyl – talk to you later, lol – laughing out loud, etc.) and thus increases message efficiency if both parties are familiar with this text language. Call takers will need to learn this text language or require the caller to type normal speech.

2. Advanced call transfers. 9-1-1 Calls will be received from potentially anywhere in the world. In the event that VoIP calls are routed incorrectly, they will need to be transferred to the correct call center. Call takers will have to make these call transfers.

3. Call takers will be required to transfer 9-1-1 callers to responder agencies so additional information can be provided by the reporting party.

4. Caller location. Caller location may not be included in the call data stream. The call taker may be required to access location databases to pinpoint callers.

5. Video/photographic triage. Call takers will be receiving pictures and videos of incident scenes and be expected to interpret what response is required for the pictured incident.

6. Advanced information gathering. Call takers/dispatchers will have additional access to information and will be expected to access this information to assist in dispatching the appropriate personnel and equipment to an incident.

7. Graphic Incident Information. Call takers will be exposed (via photos and video) to traumatic incidents and will be required to perform upon such exposure. For example, a call taker may receive a video of someone committing suicide. Call takers will require special training in order to handle these stressful calls.

8.1.2 Responders Training

Public Safety Responders will be given additional call information prior to and during incident responses. These Responders will require training to process this additional information, maintain caller privacy, etc.

8.1.3 Public Education

The public will require information regarding the NG9-1-1 system's capabilities and limitations. Figure 4 is an example of a public education flyer advising users of the limitations of the current 9-1-1 system operation.

Figure 4 Harris County (TX) 9-1-1 Public Education Flyer (front and back)

9. ESINET MANAGEMENT

9.1 ESInet Performance Requirements

The Board understands that the successful network services provider will negotiate terms and conditions for network management and performance monitoring with the Board. As a baseline, however, the Board will require any network services offered to meet certain minimum requirements, and be able to document that these requirements are met, including:

1. The services shall use a highly reliable architecture. Proposals should describe the technologies/protocols used to enhance reliability and survivability of the network.

2. The network should be designed to automatically reroute all data types around broken or failed links without manual intervention.

3. The network should be capable of prioritizing critical traffic over other traffic by user, by application, by time of day, date, or a combination of criteria. The network should support multiple levels of prioritization to ensure that the most important applications or users have the access and bandwidth that are required for successful communication.

4. The network should be capable of treating content through prioritization and bandwidth management to provide guaranteed Quality of Service (QoS). In the event of a disaster, where security and public safety applications must have priority, the network should automatically adjust QoS for prioritization.

5. The network should use traffic shaping and traffic policing to ensure that the network meets or exceeds its performance contract requirements.

6. The network should support multiple levels of authentication. In addition, the network should detect any connection that is not encrypted, and detect any node (even if spoofed) that is not authorized on the network and disallow that node from access to the network. Proposing network providers should describe the security processes and mechanisms of their proposed network. Proposals should address the following security issues.

    a) Address spoofing.

    b) Denial of service and other suspected intrusions.

    c) Undelivered packets.

    d) Physical security.

    e) Security of the information on the networks.

7. The proposed network should support secure remote access by authorized users via dial-up, DSL, cable modem, or other secure methodology.

9.1.1 MPLS Network Management

ESInet management will include the following minimum services:

1. Performance monitoring of the network.

2. Real-time and historical reporting functions that demonstrate conformance with the Service Level Agreement (SLA). Network proposals should include a complete set of sample reports that will be provided.

3. Alerting capabilities to notify technical staff and others of network outages.

4. Preventive maintenance on a regular basis as identified in the SLA.

5. Software upgrades to keep the network components up-to-date, compatible, and secure.

6. Infrastructure repair, routine, emergency and preventive maintenance, and replacement per the Service Level Agreement.

9.1.2 Network Operations Center

The MPLS network service provider should be equipped with at least one Network Operations Center (NOC). The NOC should be equipped with a Network Management System (NMS) that monitors the performance of the network and infrastructure.

1. The NMS should monitor the performance of all devices on the network, down to the demarcation point of each network link.

2. The NMS should monitor the environment at all locations where critical network components are housed, including temperature, humidity, etc.

3. The NMS should monitor ancillary network components such as power utilization, backup power systems (including generator status, fuel levels, battery condition, etc.), and equipment room security. The network service provider should identify all the monitoring points and performance metrics that will be monitored by the NMS.

4. All NMS services supporting the network should be available to the Board over a secure web-based interface. The NMS should allow up to five simultaneous users with no degradation to the network operations or performance. The NMS should allow multiple levels of access based on logon and password. (While the Board will have rights to monitor network performance and receive alarms based on specific performance criteria, nothing here is intended to relieve the network service provider of any responsibilities it has to monitor the networks and respond to network or component failures or other performance degradations. Said responsibilities should be clearly identified in the Service Level Agreement that will be executed in conjunction with the contract award.)

5. Proposing network service providers should completely describe the alarm notification services that the NMS will utilize and describe the content of the alarm notifications.

6. In addition to real-time performance monitoring, the NMS should prepare historical reports quantifying the performance of the networks (at no additional charge to the Board). Typical reports should include latency, jitter, packet loss, throughput, traffic volumes, up time, alarms received, and a description of responses and resolutions. All incidents should be time stamped. Reports should be able to be prepared on an hourly, daily, weekly, monthly, and annual basis. Trend analysis should also be included in these historical reports. Reports should be provided in electronic format to facilitate sorting and analysis of the data.

9.1.3 Service Level Agreement

The Board will be required to enter into a Service Level Agreement (SLA) with the MPLS carrier. At a minimum, the items to be included in the SLA, and recommended Board requirements, are listed below, with recommended thresholds.

1. Network availability (industry standard of 99.999% for each component is expected. Service providers should describe how they calculate availability.).

2. Packet latency (20ms).

3. Packet loss (0.1%).

4. Connection success rate for remote users (99.5%).

5. Installation intervals (for new facilities added to the network, and for upgrades or changes to existing facilities – 30 days).

6. Maintenance response intervals (The Board will identify service failures deemed to be “major failures” that will require a two-hour response time by the network service provider. All other troubles should be resolved no later than the next business day.)

7. Catastrophic incident (unplanned outages due natural and man-made causes) response time of 24 hours.

8. Number of major failures per year (no more than four).

9. Quality of Service (QoS) – Voice over IP voice quality must be maintained at a minimum Mean Opinion Score of 4.0, which is the equivalent of “toll quality”.

10. Liquidated damages or noncompliance with SLAs, including financial penalties and grounds for contract termination (amount to be negotiated).

11. Liquidated damages for non-compliant maintenance response times (amount to be negotiated).

10. LEGISLATIVE ISSUES

The unique requirements of NG9-1-1 have a significant impact on the management and legislative requirements for implementation, support, and ongoing maintenance of NG9-1-1 at the national, state, and local 9-1-1 authority levels. Many of the legacy responsibilities previously handled by telephone companies and wireless service providers may be transferred to a service provider other than traditional providers. Appropriate legislation and regulations will be developed to allow entities other than traditional telephone and wireless providers to participate in the transition.

Policy, statutory, and regulatory requirements resulting from NG9-1-1 fall into the following areas:

1. ESInet – The ESInet should be managed and administered at a statewide level. Regional ESInets are optional. However, a state level, statewide ESInet is a core requirement for NG9-1-1. A public state level board, agency, or department should be authorized and enabled to plan for, implement, administer, and maintain the ESInet.

   A plan for the development and implementation of a statewide ESInet should be created, discussed, and approved by the appropriate legislative bodies. Funding should be procured through multiple funding opportunities including grants and/or from direct appropriations in order to fund the implementation of the network components (routers, switches, hubs, etc.).

   The ESInet will require administration on a daily basis, either by an entity (board, commission, agency, or department) or via outsourcing to several vendors/service providers specializing in such technologies. In both cases, daily decisions as well as short and long-term policies regarding the ESInet should be made in an equitable and fair manner. For example, equal access to the ESInet should be ensured. Conflicting objectives and limited budgets will require conflict resolution and consensus building, which are best performed based on enabling legislative rules and regulation through a public, transparent process.

   The ESInet will not be a static network. Proper bandwidth, reliability, and availability of the ESInet should be properly planned and fully functional when initially implemented. However, the bandwidth requirements, policies, and procedures governing the ESInet are guaranteed to change over time. Authority to support and maintain the ESInet, which will become a critical emergency system component, should be vested in a public body in order to ensure its proper operation over time.

   NG9-1-1 Applications, Policy Rules, and Data – There are certain applications and associated databases that should be coordinated at a state level. Emergency requests that are initially routed in error ending up at neighboring or distant PSAP, should be redirected to the appropriate PSAP within the Commonwealth, will utilize the statewide ESInet, which will then use the ECRF to determine which specific PSAP within the

Commonwealth should handle the emergency request. An emergency request that originates at one PSAP, but is destined for a different PSAP will normally be routed to the proper PSAP through the statewide ESInet and the ECRF. The Emergency Request Routing Proxy (ECRP), residing on the Statewide ESInet, will determine the address for the PSAP or regional ESInet to which the emergency request should be routed.

Legacy network gateways that support wireless service providers and the PSTN will reside either at the edge of, or within the regional ESInet. It will be too cumbersome and expensive for service providers (ILECS, LECS, wireless, VoIP, etc.) to connect to every PSAP within the Commonwealth. There will be redundant and highly available connections designed from these service providers to the statewide ESInet, which will then be responsible for routing emergency requests received from these providers to the appropriate PSAP and then on to the appropriate emergency responders.

All of these applications, as well as the NG9-1-1 applications that reside at the PSAP level will require policies, procedures, and data to accomplish their activities. It is critical that these databases are populated with policies, procedures, and data that are coordinated statewide and that meet NENA and other NG9-1-1 standards.

A public state level board, agency, or department should be authorized and enabled to maintain the appropriate applications, standards, and data.

2. GIS data – The responsibility for the creation, maintenance, and update of current, accurate, and complete GIS data required for the operation of the ESInet and NG9-1-1 applications is the responsibility of the local 9-1-1 authority. The local 9-1-1 authority will have to develop the staffing, acquire the GIS equipment and services, train the staff, and otherwise arrange for the initial creation and continuous, timely update of the GIS data required by the locally resident (within the PSAP) and ESInet resident NG9-1-1 applications. The data quality, content, and currency must meet NENA and other standards and must be readily available in a standard data exchange format to be used by the NG9-1-1 applications.

   Funding and authority will have to be vested with the local 9-1-1 authority to enable the development of the required GIS data. In addition, a state and/or regional level agency will have to be vested with the authority to ensure that the data conforms to established NG9-1-1 standards and maintenance procedures. In addition, a collaborative procedure will have to be undertaken by the local PSAPs and managed at a state or regional level entity to fix any identified boundary and other GIS data discrepancies (e.g., boundary overlaps and coverage gaps between polygons).

   It is critical that all applications utilize the same GIS data to validate location data and to route emergency calls. Otherwise, a looping situation can develop in which one entity believes that the call belongs in a different PSAP and the other PSAP believes that the call belongs in the original PSAP. Under this circumstance, the network will pass the

call back and forth in a potentially endless loop until someone discovers or fixes the discrepancy. Regional and state level coordination is required to ensure that all GIS data conforms to topological and other requirements.

3. Coordination and Control – Not all 9-1-1 authorities across the state will be able to simultaneously develop the required expertise and data, along with obtaining the funding necessary to upgrade to NG9-1-1. Coordination and control of the transition effort must be vested in a state level entity in order to ensure conformance with established ESInet standards, to establish uniform standards and mandates, to certify compliance of individual PSAPs with mandated requirements prior to cutover, and to develop funding mechanisms to support the transition.

4. Discrepancy resolution – GIS and other data for different PSAPs must be coordinated. Identified discrepancies should be brought to the Board's attention. Regional and/or state level entities must be vested with the authority and funded to resolve discrepancies between PSAPs and to coordinate the correction of the discrepancies.

The Board has reviewed the Kentucky Revised Statutes (KRS) and Administrative Regulations (KAR) to determine their adequacy for supporting future Next Generation (NG9-1-1) and current ESInet standards and requirements. In addition to the regulation and legislation, the Board also used various National Emergency Numbering Association (NENA) policy documents and emerging 9-1-1 standards developed by NENA, Internet Engineering Task Force (IETF), and the Alliance for Telecommunication Industry Solutions (ATIS) for the development of the recommendations for the modification of the current statutes and administrative regulations.

The NG9-1-1 Standards Report (Appendix B), goes into the details of all the enabling legislation (Kentucky Revised Statutes) related to 9-1-1 emergency request reception and processing in the commonwealth of Kentucky and the Kentucky Administrative regulations related to 9-1-1 emergency request reception and processing and to the CMRS Board that were reviewed. The NG9-1-1 Standards Report also presents the recommended modifications to be considered as the Commonwealth transitions to a full NG9-1-1 capable system.