# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

As part of the NG9-1-1 Project Consultant services for the State of Ohio (State), L.R. Kimball provides the State with alternative options for statewide implementation and operation of an Emergency Services IP Network (ESInet). ESInets are an IP-based, network of networks that are designed to share call information with other public safety agencies. Communications technologies of today and tomorrow require a highly standardized system capable of delivering voice, video, images, text, and telematics as well as emerging technologies over broadband, packet switched technology capable of carrying large amounts of data. Internet Protocols (IPs) and the National Emergency Number Association (NENA) standards, are used to engineer hierarchical managed networks to deliver emergency call services.

L.R. Kimball has discussed the options along with gaps and areas of concern with the committee to determine the design which best suits the needs of the State. It is recognized that locations within the State already support regional or countywide ESInets or are in the process of designing networks for their area's emergency services functions. The design of the Statewide ESInet must support ease of connectivity for regional ESInets, as well as individual Public Safety Answering Points (PSAPs) to connect.

The methodology used to compile these recommendations was a collaborative effort between the State of Ohio ESInet Steering Committee, the State of Ohio 911 Program Office, OARnet, and key representatives of public safety in Ohio. The initial design is based on a consensus of the Committee and other relevant stakeholders to develop the system's technical, implementation, and operational requirements.

The remainder of this page is intentionally left blank.

# 1. OHIO NEXT GENERATION 9-1-1 CORE FUNCTIONALITY

The logical and functional design provides the information required to begin discussing the functionality of the network. A high-level next generation 9-1-1 (NG9-1-1) conceptual design that is consistent with NENA i3 standards is depicted below. This diagram does not depict every possible interconnection arrangement. Multiple instances of some functions may be deployed at various locations. For example, some originating networks may supply their own Legacy Network Gateways (LNGs), and additional LNGs may be deployed in the statewide core services cloud.

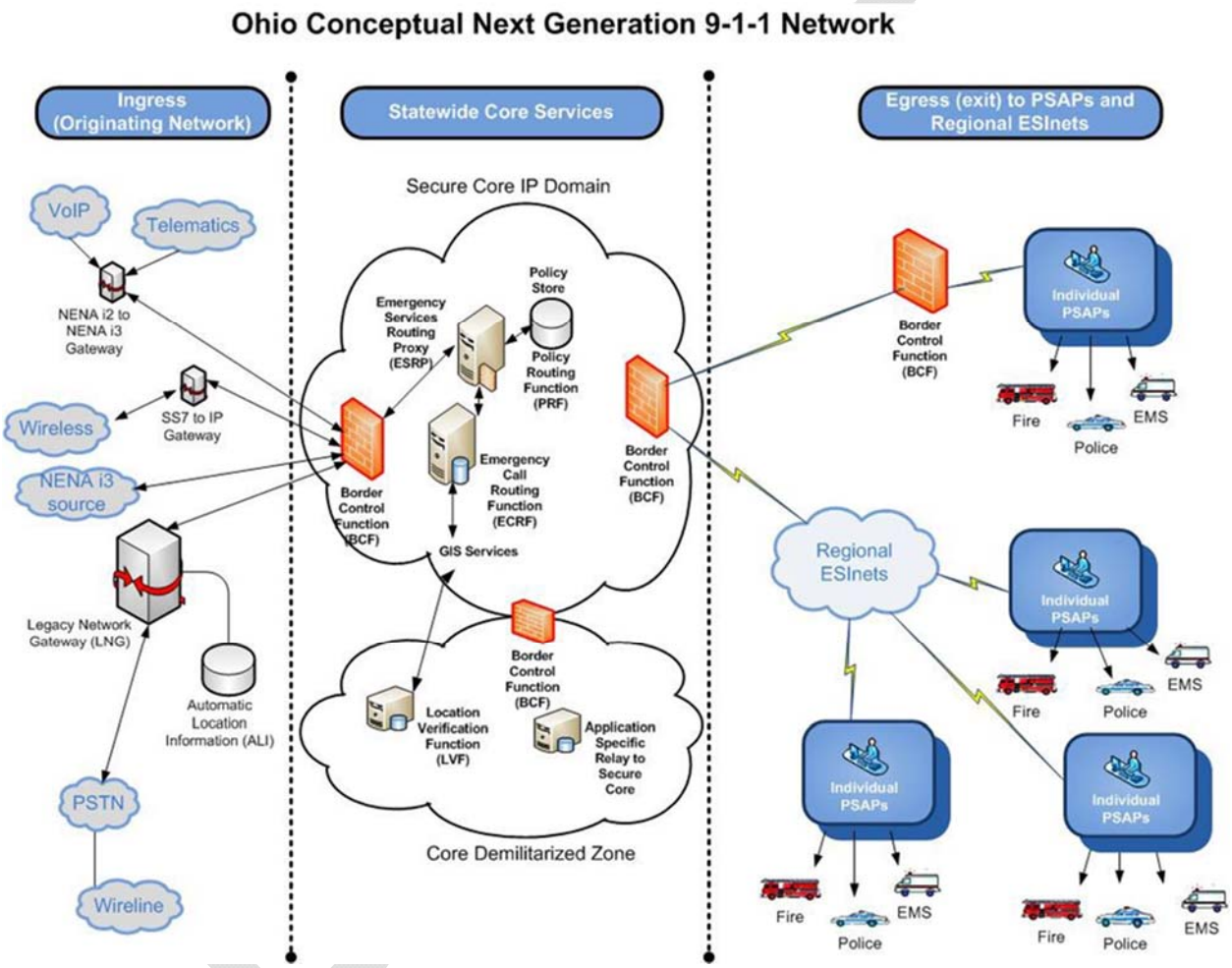


**Figure 1—Ohio Conceptual Next Generation 9-1-1 Network**

L.R. Kimball discussed this conceptual design with the stakeholders to refine the desired design functionality of the statewide ESInet to determine the design best suited for Ohio. Design and functionality include:

- Ingress Originating Network
- Statewide Core Services
- Egress to PSAPs and Regional ESInets

## 1.1 Ingress – Originating Network

This section includes components to consider for the composition of the originating call network.

- Voice over Internet Protocol (VoIP) and Telematics – includes all originating calls that do not fall under traditional wireless and wireline calls. L.R. Kimball recommends Ohio require calls to be delivered per NENA i3 standards which may require the provider to translate NENA i2 to NENA i3 prior to the call being sent to the statewide ESInet.
- Wireless – includes traditional wireless calls originating from a cellular phone users. Current delivery holds the expectation that the provider deliver the call via a Signaling System 7 (SS7) to IP gateway.
- Wireline – This includes traditional wireline calls delivered by Local Exchange Carriers (LEC). A LEC may provide and operate their own LNG and deliver the calls in the NENA i3 format, or the State may provide LNGs to terminate legacy 9-1-1 trunks and ALI circuits. The State should consider whether to require LECs to deliver emergency calls in i3 format.
- Originating calls and the format required by the carrier(s) and other providers as well as the methods and systems desired for the Ohio Statewide ESInet still need to be discussed and determined.

## 1.2 Statewide Core Services

The State will provide core services within the statewide ESInet. These are services that are generally provided to route and deliver calls. Core services provided within the statewide ESInet range in variety from state to state and are customized to meet the needs of each. Ohio core services will be provided along with an ESInet backbone provided by OARnet. Core service providers will be required to locate their serving equipment in a state provided data center. PSAPs across the State will have the following options for connecting to statewide core services.

- Full services - includes core services and hosted remote CPE from the State
- State core services - PSAP owned CPE
- State core services – Regional/County owned interoperable PSAP core services

A State pilot host environment test bed is currently underway in Hamilton County with additional counties set to join.

Based on feedback collected from Ohio PSAPs, this section lays out core services are that are important to the PSAP community to have available on the statewide ESInet.

### 1.2.1 Border Control Functions (BCF)

The border control function begins with a firewall to protect the statewide ESInet from malicious activity from the originating call providers at the point of ingress and from PSAPs, regional ESInets or other services with access to the statewide core services. Other border control functions may include verifying the call information configuration and/or translation among various call formats and protocols.

### 1.2.2 Emergency Services Routing Proxy (ESRP)

The ESRP is where the call information is processed and then subsequently delivered to the appropriate PSAP or regional ESInet. Included within this function:

- Policy Routing Function and the Policy Store – determines if the PSAP or Regional ESInet is available to receive the call or if alternate or special call routing is required.

### 1.2.3 Geographic Information System (GIS) Services

A GIS database and associated tools which is used by the ECRF to determine the most appropriate PSAP and/or emergency responders associated with a specific location, either latitude and longitude, or a civil address. . Geographic Information System services are at the discretion of the state and are generally dependent upon the existence of an existing GIS database.

### 1.2.4 Location Validation Function (LVF)

The location validation function provides a means whereby authorities, service providers, and other stakeholders can pre-verify that an address is of the correct form, is valid with respect to the GIS database, and returns PSAP and first responder information appropriate to that location. For example, LECs can use the LVF to verify addresses in their legacy ALI systems will be correctly routed by the NG9-1-1 system. An LVF instance may be a Statewide Core function which uses the same GIS data that is used by the ECRF. However, such an LFV must be made available to users outside the Core Services cloud while the ECRF is used in real time by processes that handle live emergency calls. Hence, the LFV and ECRF functions have different security requirements.

### 1.2.5 Emergency Call Routing Function (ECRF)

The ECRF is a functional element in a NG9-1-1 system which associates a location with a call destination using GIS data. An instance of the ECRF is the Location to Service Translation (LoST) protocol server where location information (either civic address or geo-coordinates) and a Service Universal Resource Name (URN) are the input to a mapping function which returns a Uniform Resource Identifier (URI) used to route an emergency call toward the appropriate PSAP for the caller's location or towards a responder agency.

### 1.2.6 Legacy Network Gateway (LNG)

The LNG is a signaling and media interconnection appliance between legacy wireline/wireless originating networks and the NG9-1-1 ESInet. A LNG may convert legacy ALI to NENA i3 location. LNGs may be provided by the originating network operator, the State, a PSAP, or in any combination as desired and required.

## 1.3 Egress to Public Safety Answering Points and Regional Emergency Services IP Networks (OARnet)

The call is delivered from the statewide core services to the PSAP or regional ESInet. Additional BCF may exist at the point of ingress to the PSAP or regional ESInet. These functions may vary according to the needs of the receiving location and the decisions of Ohio. PSAPs with only legacy equipment will require a Legacy PSAP Gateway (LPG), which performs the inverse function of an LNG, to convert the NENA i3 format back to legacy formats. The main goal is to deliver the call in a format consistent with the receiving location's capabilities. Confirmation and possible changes to formatting are at the discretion of the State.

The remainder of this page is intentionally left blank.

# 2. STATEWIDE EMERGENCY SERVICES IP NETWORK DESIGN (OARNET)

It is the goal of the State of Ohio 911 Program Office to provide an ESInet that spans the state providing NG9-1-1 services to all 88 counties within the State utilizing OARnet as the backbone for the ESInet. There are 13 Points of Presence (POPs) distributed across the state to provide access to three fiber rings operating at 10 gbps per ring. Current OARnet connectivity is demonstrated in the following diagram.

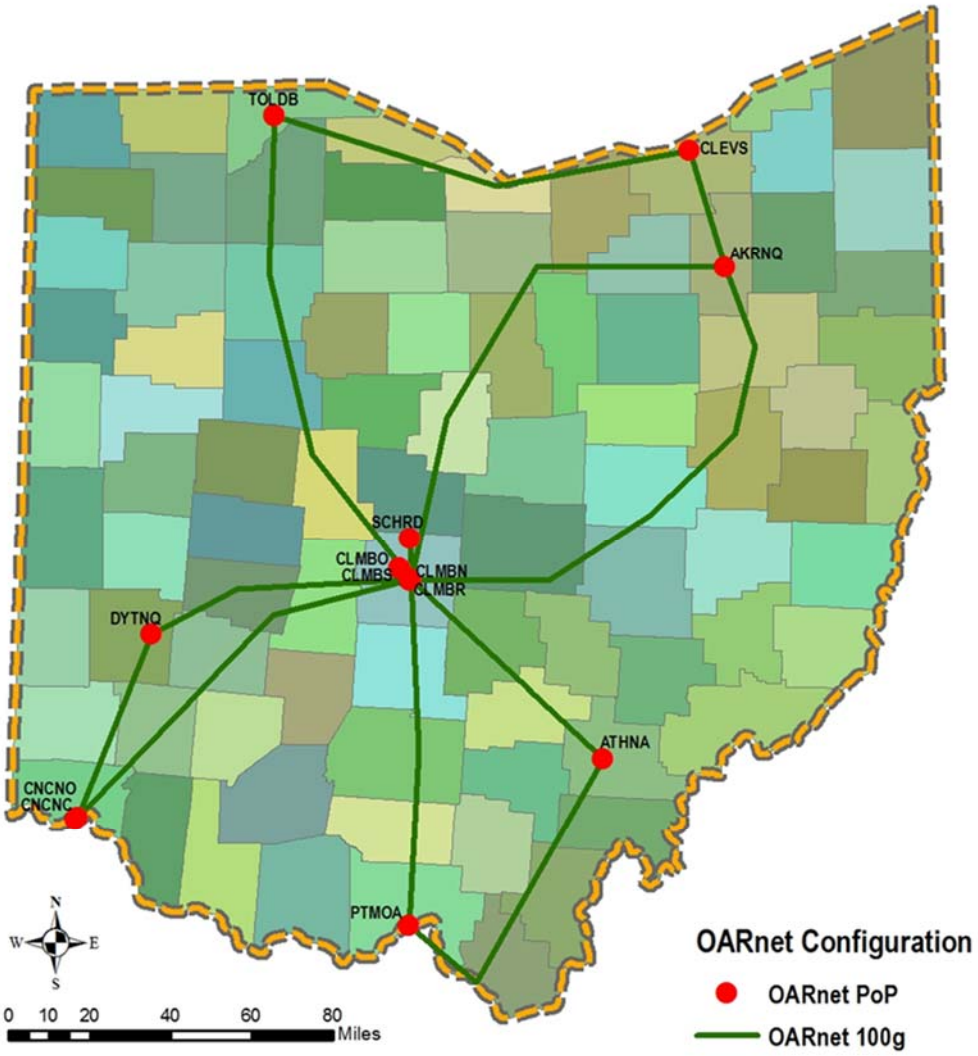


**Figure 2 – OARnet Connectivity**

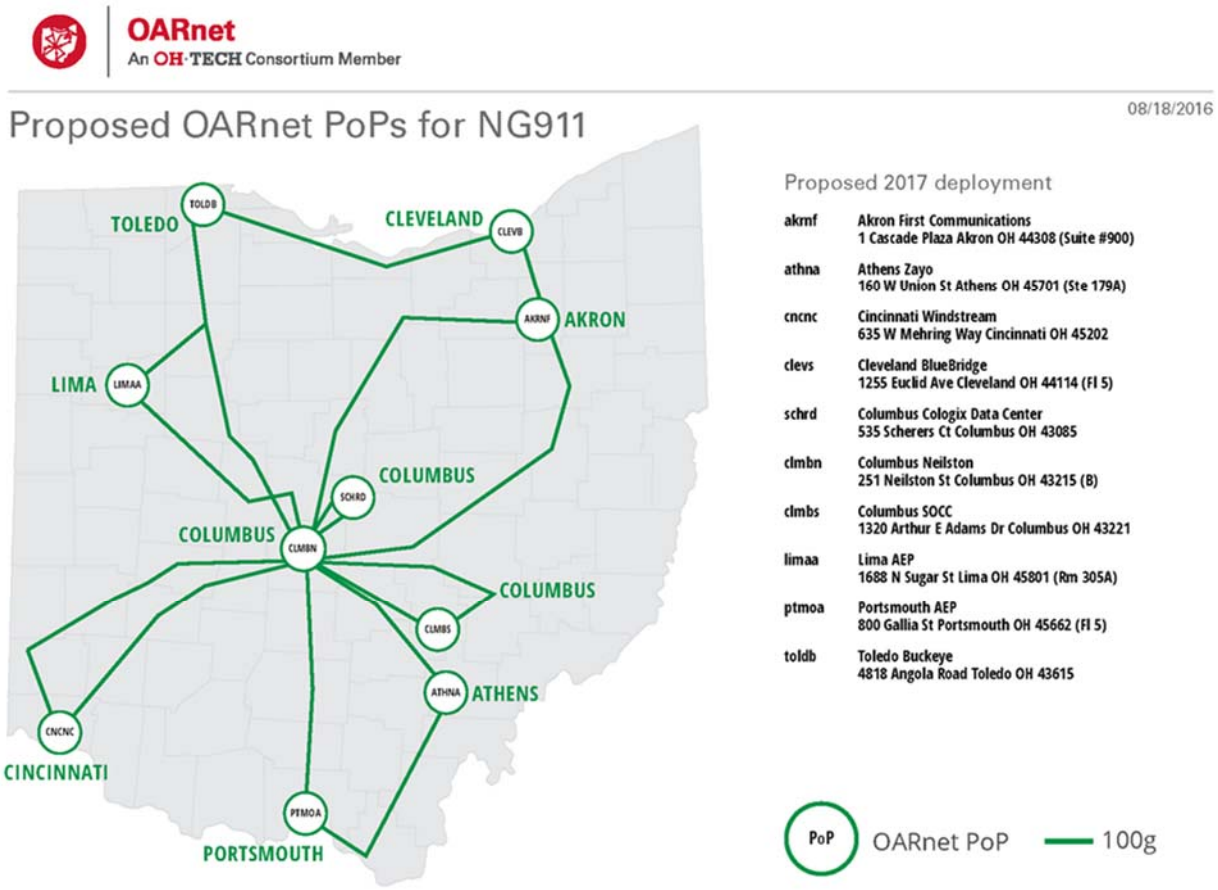


**Figure 3 – Proposed OARnet PoPs for NG9-1-1**

## 2.1 Service Level Objectives

OARnet has provided L.R. Kimball with the following service level objectives for this report:

- Network Availability: 99.999% for Protected Service and 99.99% for Unprotected Service. (Note: Service is considered unavailable when there is a complete loss of use.)
- Mean Time To Repair (MTTR): Yearly average of two (2) hours per occurrence with no single occurrence lasting more than four (4) hours from the time a Trouble Ticket is opened.
- Mean Time To Response (MTTRe): Yearly average for response to call 5 minutes to enter trouble ticket, and one hour updates if needed.
- Latency: 18 ms one way/ 36 ms round trip
  Latency objective is measured as the average sample taken during a 30 day period between network terminating equipment to which the ports are assigned.

- Packet Delivery Rate: 99.9%
  Packet Delivery Rate objective is calculated as the total number of effective Ethernet frames, per port that successfully traverse the network divided by the total number of effective Ethernet frames per port offered to the network within a 30 day period.
- Jitter: 20ms
  Jitter is calculated as the delay variance of the packets transported across the network or delta of delay between two consecutive packets by averaging sample measurements taken during a 30 day period between network terminating equipment.
- Protocol's Supported: IPV4 and IPV6

OARnet meets or exceeds the current standards for Next Generation requirements for Availability, Latency, Jitter, supported Protocols, and Packet Delivery but are not well defined in the areas of MTTR and MTTRe. OARnet SLA's must be better defined to meet NENA i3 technical standards and operational requirements as written in this document.

## 2.2 Design Options

The State of Ohio 911 Program Office has indicated that all 88 counties must have access to a statewide ESInet. In most cases, bandwidth needed determines how ESInets are designed. L.R. Kimball is proposing two options to provide the PSAPs of Ohio, at the very least, the ability to accept IP-based i3 communications over an IP network.

### 2.2.1 Option 1

Design the bandwidth requirements in what has been called "the bottom up" method.

- Remote PSAP - Controller = 1 mbps (for the PSAP as a whole) + 100 kbps x number of positions.
- Controller – Gateway/Core Services = 144 kbps x number of 911 trunks.

L.R. Kimball has had discussions with 9-1-1 CPE manufacturers and have seen this proposed for other statewide Next Generation 9-1-1 deployments, but this option is designed with the bare minimum bandwidth capable of handling voice and text. This design would require the network to also be scalable to handle video, images, telematics, and future technologies. An in service upgrade will need to be planned and implemented with the possibility of a service interruption.

### 2.2.2 Option 2

Design the bandwidth requirements according to NENA standards[1] for IP Network Design.

- Remote PSAP - Controller = 2 mbps (for the PSAP as a whole) + 2 mbps x number of positions.
- Controller – Gateway/Core Services = Sum of bandwidth of all PSAPs served by a controller.

This design option would provide enough bandwidth to handle voice, text, video, images, telematics, and position the State for future technologies. Service upgrades to increase bandwidth should not be needed reducing the possibility of any service interruptions. Option 2 would be the preferred option and would depend on the capacity of OARnet.

[1] NENA 08-506 v1

## 2.3 Analysis

In an effort to compile a comprehensive and realistic report, L.R. Kimball worked with OARnet and other key personnel within the State of Ohio to obtain current operational characteristics of the network and identify any potential deficiencies. OARnet currently does not have direct access to all 88 counties in the State. There are two methods to access the public safety POPs:

- Negotiated contracts with network providers across the state, not all providers provide public safety grade services in all of their coverage areas.
- Customer provided fiber facilities.

As a value added service, OARnet will provide network monitoring and maintenance. Some locations have OARnet provided network devices to facilitate monitoring.

OARnet does not have a structured list of county by county providers available to offer ESInet facilities due to different service levels available throughout their serving areas. OARnet has offered to provide coverage maps and a more detailed list of providers once PSAP addresses (GPS coordinates) can be provided.

The remainder of this page is intentionally left blank.

# 3. STATEWIDE CORE SERVICES INTEROPERABILITY

The State of Ohio 911 Program Office has developed a NG9-1-1 Plan to provide NG9-1-1 services to all PSAPs within the State of Ohio. The plan provides 9-1-1 services based on the needs and services required by individual PSAPs and 9-1-1 Regions.

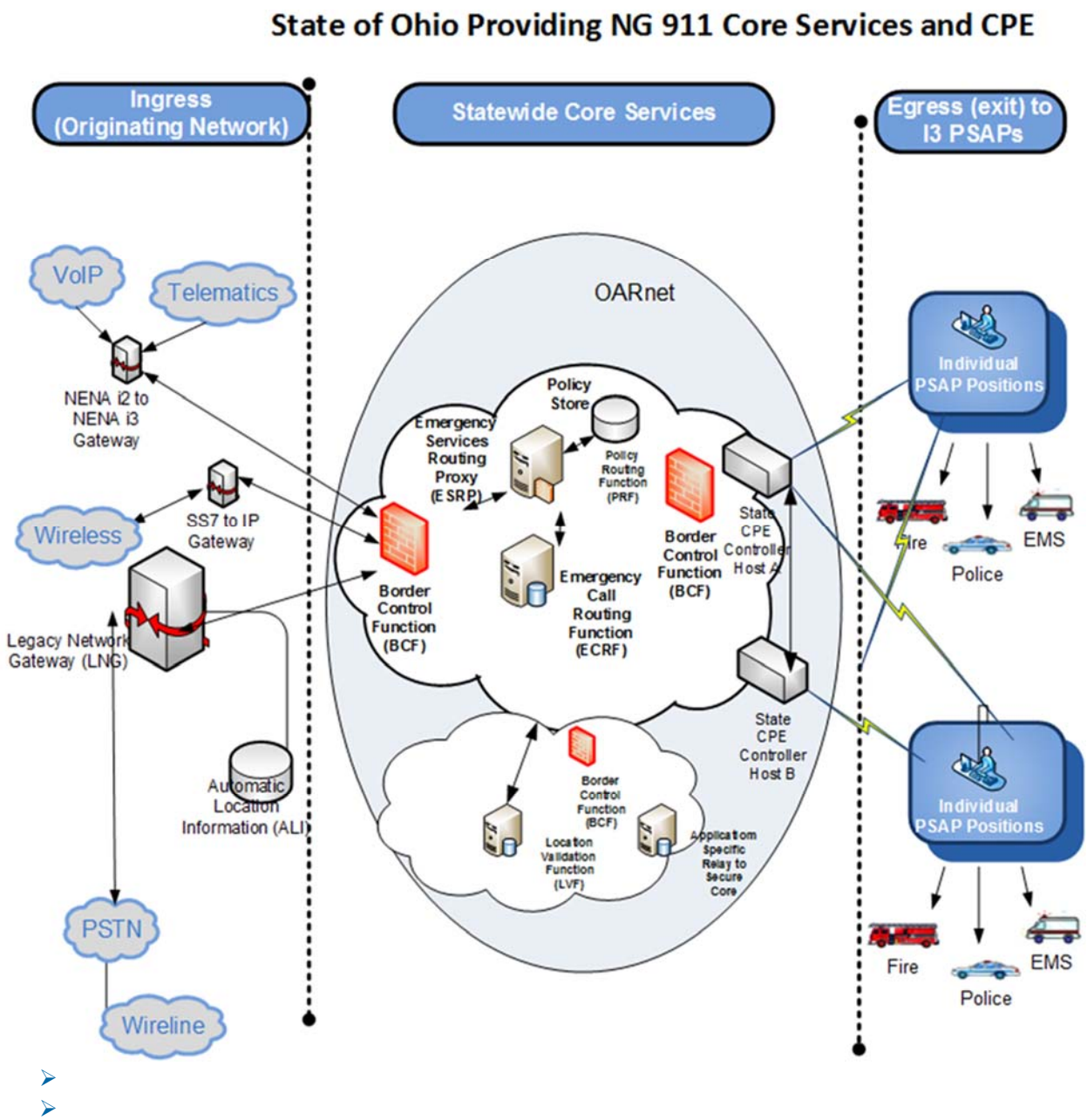


**Figure 4 – State provided core services and CPE.**

## 3.1 NG9-1-1 Core Services to Independent PSAPs or Independent Region

The State of Ohio 911 Program Office will provide NG9-1-1 core services to PSAPs wishing to maintain their own individual controllers (CPE). The PSAPs will have the ability to connect their individual i3 compliant controllers or regional i3 compliant controllers to the State provided core services. While these independents will have the ability to choose their own i3 compliant controllers, the state will provide the core services. This will provide these individual PSAPs or individual Regions interoperability with other PSAPs using the State provided core services as shown in Figure 5.

The remainder of this page is intentionally left blank.

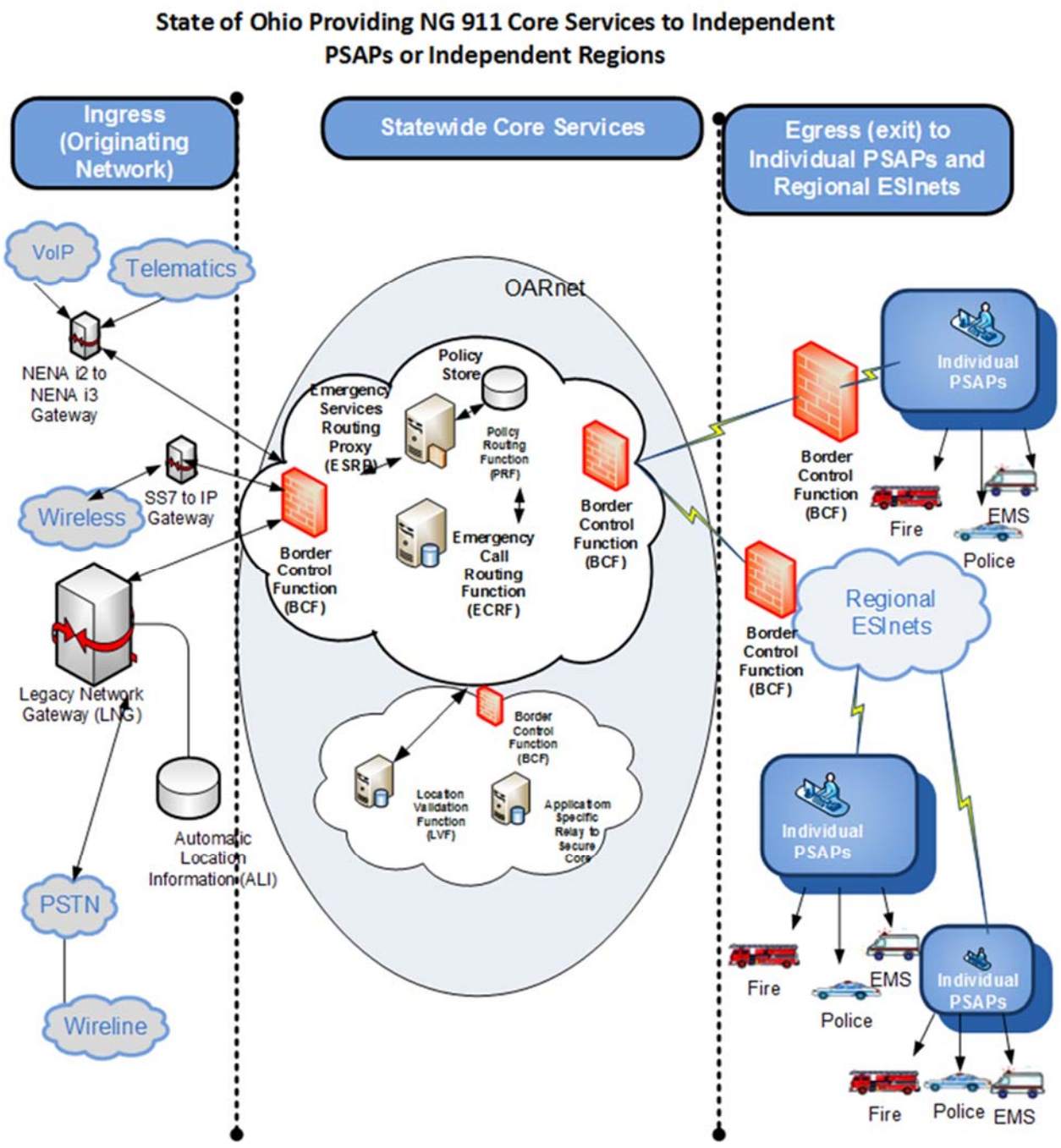


**Figure 5 -- State provided core services to independent PSAPs and Regions.**

## 3.2 NG9-1-1 Core Services providing Interoperability with Independent Core Services

The State of Ohio 911 Program Office will provide NG9-1-1 core services for those PSAPs and Regions that have established independent core services. This will provide the ability for those PSAPs using the independent core services to have interoperability with all PSAPs connected to the State provided core services. Providing this, allows other ESInets to have NG9-1-1 call functionality with others, whether it be core service within the state or interstate networks as shown in Figure 6, below.

The remainder of this page is intentionally left blank.

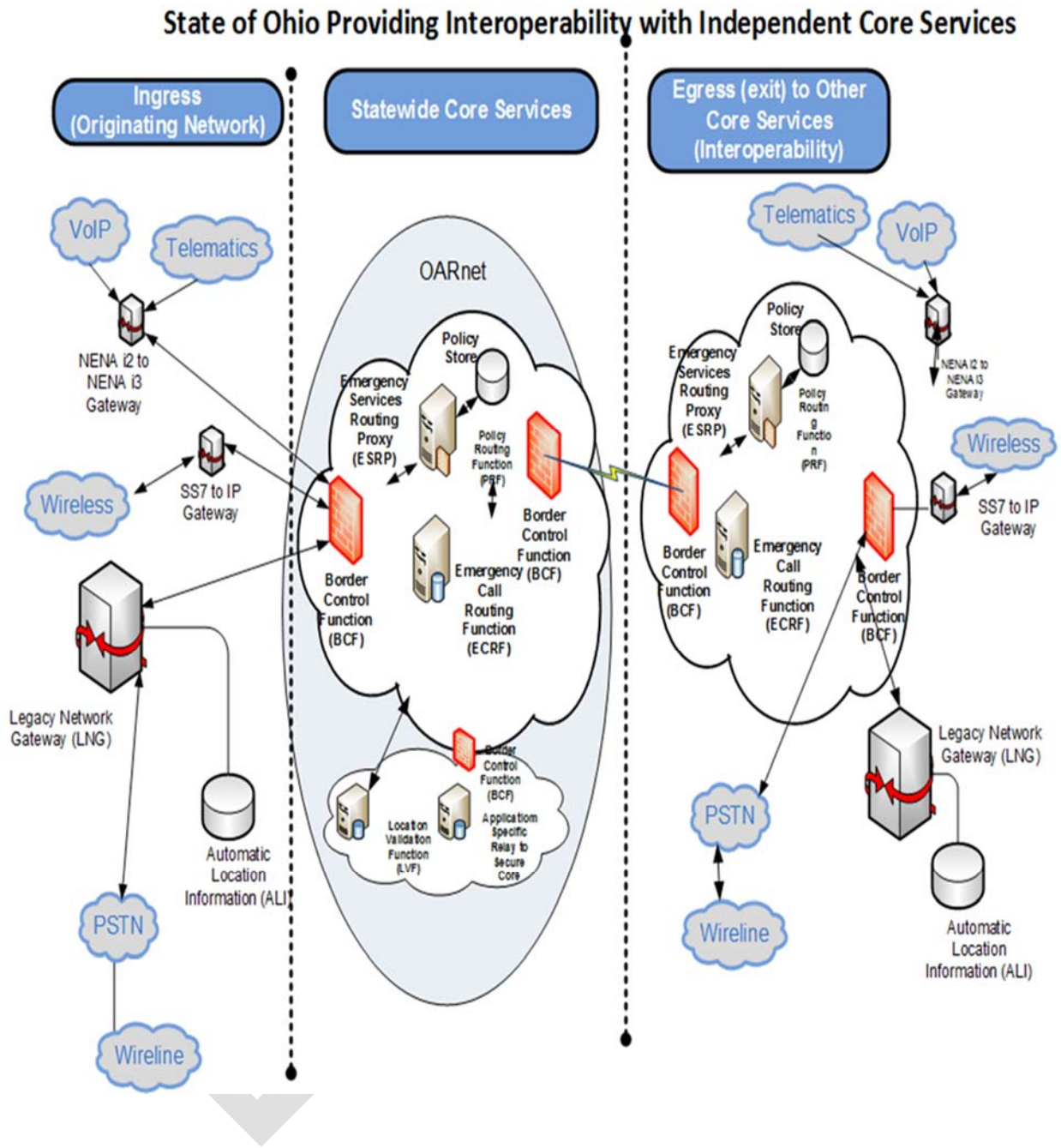


**Figure 6 – State provided interoperability with independent core services.**

# 4. DATA NETWORK TRANSPORT REQUIREMENTS

The following sections describe the requirements for the Data Network Transport supporting the design of the State ESInet. These sections represent the technical, operational, and functional requirements that must be satisfied.

## 4.1 Multi-protocol Label Switching (MPLS)

MPLS is a major component of the State ESInet. MPLS is a data communications platform that emulates the features of a circuit-switched network over a packet-switched network. The MPLS must support routers and gateways from multiple manufacturers since this network will be used for multiple public safety applications. If the vendor's solution includes multiple MPLS networks, each network must be identified. OARnet must provide the committed bandwidth rates. MPLS security is a concern; OARnet must provide SLAs specifying and addressing security on the MPLS networks, including detailed specifications on how they plan to handle security, use of internal security reviews, testing, and mechanisms used.

## 4.2 Network In-service/Uptime Requirements

The network developed for this project needs to be a public safety grade network requiring 99.999 percent availability or better.

## 4.3 Gigabit Ethernet – Network Core Bandwidth Requirements

Core host network interconnections must have a minimum committed information rate (CIR) of 1 gigabyte per second (Gbps) between all network devices. All network edge devices must support a minimum of 100 Mbps.

## 4.4 Gigabit Ethernet Transport Requirement to hosts

Gigabit Ethernet Transport must interconnect all core hosts in the State ESInet. A host can consist of IP servers and gateways, Instant Messaging (IM) servers, Short Message Service (SMS) servers, or systems supporting future emergency requests, such as images or video. The Gigabit Ethernet Transport shall be used for data-centric emergency requests, IP call signaling, media transport, server signaling, network management, monitoring and alarms.

## 4.5 Redundant Gigabit Connections to the host

All core hosts must have redundant gigabit links or logical connections. Redundant gigabit connectivity must ensure no single point of failure exists and contribute to maintaining the 99.999 percent availability requirement. The redundant gigabit link shall be placed into a separate hardware switch device than the primary gigabit link to ensure redundancy. A separate power supply source for the redundant gigabit switching device is also required.

## 4.6 Redundant Gigabit Connections Load Sharing

To ensure the redundant gigabit links or logical connections are operational and can support data transactions, the design must support load sharing when both links are available or in service. All links and network devices must support this design.

## 4.7 Gigabit Ethernet–Committed Information Rate (CIR)

A CIR on a proposed Gigabit Ethernet of one Gbps must be provided for each of the host locations.

## 4.8 Network Devices

The network design requires that core network devices and equipment be redundant to ensure 99.999 percent reliability and that no failure of a link or device totally isolates the core network. A fail-over must be transparent, automatic and ensure continued, uninterrupted operation of emergency service applications or any service request currently in progress.

The State ESInet must be designed such that the failure of any one network module will not result in total system failure, nor result in blocked, dropped or busy calls. Only the loss of the equipment or connectivity associated with that module should be affected. Any failure resulting in the use of the public switched telephone network (PSTN) must not increase current call setup times. The network provider must test and document this requirement.

OARnet must describe and diagram the network architecture with respect to the major components or modules, and must provide a call-flow diagram describing how the entire system will react to a failure of each major component or module.

## 4.9 Remote Location Bandwidth Requirements

Ethernet connections from the core network to the remote workstations must be a minimum of 100 Mbps. All edge network devices must support this bandwidth requirement.

## 4.10 Megabit Ethernet – CIR

A CIR on the Megabit Ethernet of a minimum of 10 Mbps must be provided for each remote workstation from the core network.

## 4.11 Network Disaster Recovery

The network must be designed to include a disaster recovery plan for partial or total loss of the State ESInet (either transport or network devices) and/or loss of connectivity to remote workstations.

## 4.12 Security

The network design must include network security management policies and procedures in sufficient detail to ensure confidence that the State ESInet is not vulnerable to unauthorized activity or unauthorized access that would degrade public safety operations.

The remainder of this page is intentionally left blank.

# 5. RECOMMENDATIONS

L.R. Kimball recommends the State of Ohio 911 Program Office move forward with Design Option 2 to prepare an ESInet backbone for statewide connectivity, over a network with the built in capacity to handle text, video, social media, telematics, and future technologies as they are introduced. The ESInet needs to be designed to meet or exceed NENA i3 technical standards. It is important that the State continue to provide leadership and move forward with their vision of utilizing IP-based networks to interconnect Ohio's Public Safety system.

The remainder of this page is intentionally left blank.