

Report for

ESInet Technical and Operational Requirements



Prepared for

Ohio Department of Administrative Services

November 2013 ©



L.R. Kimball®
TARGETED RESULTS. EXPERTLY MANAGED.
WE STAKE OUR REPUTATION ON IT.

A CDI Company



ARCHITECTURE • ENGINEERING • COMMUNICATIONS TECHNOLOGY
AVIATION | CIVIL | CONSTRUCTION SERVICES | DATA SYSTEMS | ENVIRONMENTAL
FACILITIES ENGINEERING | GEOSPATIAL | NETWORKS | PUBLIC SAFETY | TRANSPORTATION

TABLE OF CONTENTS

EXECUTIVE SUMMARY	2
1. OHIO NEXT GENERATION 9-1-1 CORE FUNCTIONALITY.....	3
1.1.1 Ingress – Originating Network	4
1.1.2 Statewide Core Services	4
1.1.3 Egress to Public Safety Answering Points and Regional Emergency Services IP Networks	5
2. STATEWIDE EMERGENCY SERVICES IP NETWORK DESIGN	6
3. STATEWIDE EMERGENCY SERVICES IP NETWORK REQUIREMENTS AND SPECIFICATIONS.....	7
3.1 EMERGENCY SERVICES IP NETWORK REQUIREMENTS	7
3.1.1 Next Generation 9-1-1 Network Backbone	7
3.2 EMERGENCY SERVICES IP NETWORK OPERATIONAL SPECIFICATIONS	24
3.2.1 Managed Network Services.....	25
3.2.2 Network Configuration and Change Management.....	29
3.2.3 Security Monitoring and Management.....	30
3.2.4 Monitoring, Alarming, and Trouble Reporting.....	30
3.2.5 Security.....	30
4. OHIO GEOGRAPHIC INFORMATION SYSTEM	32
4.1 GEOGRAPHIC INFORMATION SYSTEM STANDARDS	32
4.2 SYNCHRONIZATION OF GEOGRAPHIC INFORMATION SYSTEM DATA WITH MASTER STREET ADDRESS GUIDE AND AUTOMATIC LOCATION IDENTIFICATION DATABASES.....	33
4.3 DATA PROVISIONING AND INTEROPERABILITY.....	34
4.4 EMERGENCY CALL ROUTING FUNCTION AND LOCATION VALIDATION FUNCTION	34
4.5 GEOGRAPHIC INFORMATION SYSTEM DATA READINESS CHECKLIST	35
4.6 GEOGRAPHIC INFORMATION SYSTEM DATA LAYERS.....	35
5. RECOMMENDATIONS.....	37

EXECUTIVE SUMMARY

Emergency Services IP Networks (ESInets) are designed to provide ease of call flow with the ability to share call information by utilizing broadband, packet switched technology capable of carrying voice, plus large amounts of varying types of data. With the use of Internet Protocols (IPs) and the National Emergency Number Association (NENA) standards, ESInets are engineered, managed networks that are hierarchical, or a 'network-of-networks' supporting local, regional, state and national arenas to deliver emergency call services.

Before an ESInet is procured, it is necessary to determine the design which best suits the needs of the State of Ohio (State). It is recognized that locations within the State already support regional 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 for regional ESInets, as well as individual Public Safety Answering Points (PSAPs) to connect. Additionally, the ESInet specifications identified in this document may be utilized by all PSAPs regardless of the mode for IP connection. Ohio should also formally identify the Ohio 9-1-1 Coordinating Entity to undertake these activities.

With the initial existing infrastructure review complete, L.R. Kimball is collaborating with the State of Ohio to determine the design for the Statewide ESInet and establish Statewide ESInet requirements and specifications.

The methodology to compile these recommendations was a collaborative effort between the State of Ohio ESInet Steering Committee, the ESInet Technical Subcommittee, the ESInet Operational Subcommittee, stakeholders across the State, and L.R. Kimball. A focus group meeting was held on August 1, 2013 to examine expectations throughout Ohio and obtain input into what the Statewide ESInet should provide to entities that choose to connect. The information collected at this meeting was utilized in the compilation of these technical requirements.

The balance 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. At this point in time, the State has not decided if and which Next Generation 9-1-1 (NG9-1-1) core functions will be provided at the State level for use by the PSAPs throughout Ohio. A high-level 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.

Ohio Conceptual Next Generation 9-1-1 Network

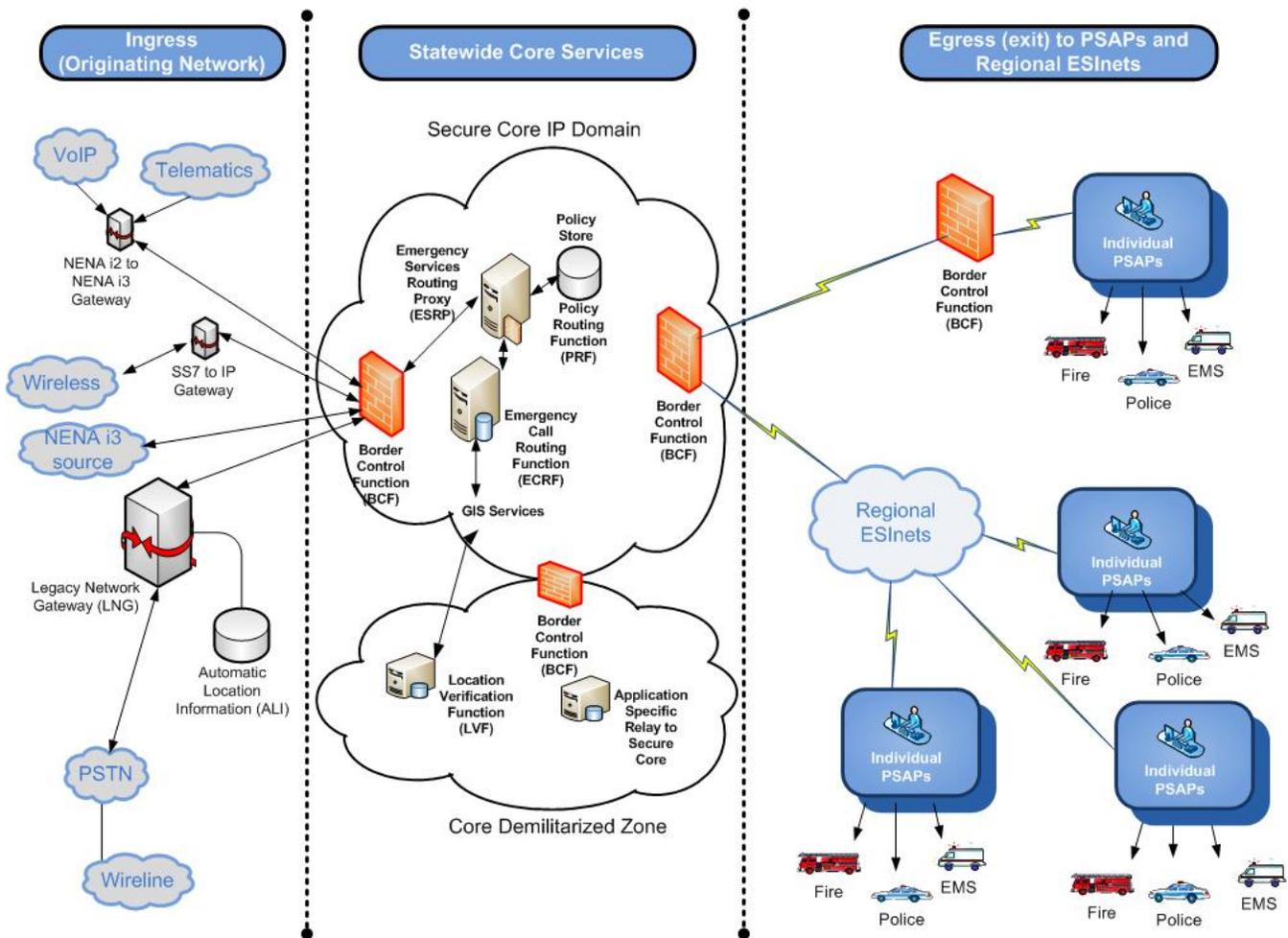


Figure 1—Ohio Conceptual Next Generation 9-1-1 Network

L.R. Kimball discussed this conceptual design with the Ohio 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

1.1.1 Ingress – Originating Network

Components to consider for the composition of the originating call network include:

Voice over Internet Protocol (VoIP) and Telematics – includes all originating calls that do not fall under traditional wireless and wireline calls. Currently, VoIP and telematics calls could be delivered via the NENA i2 standards as the NENA i3 standards are recent for these types of calls and not yet widely utilized. 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 will be discussed with Ohio to determine the methods and systems desired for the Ohio Statewide ESInet.

1.1.2 Statewide Core Services

Ohio should consider the core services that can be provided 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 has not yet decided what core services or functions they will provide along with the ESInet backbone. This will be a decision based on cost and needs of PSAPs across the State. Based on feedback collected from Ohio PSAPs, the following core services are important to the PSAP community to have available on the statewide ESInet:

Border Control Functions (BCF) – this 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.

Emergency Services Routing Proxy (ESRP) – this 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.

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.

Location Validation Function (LVF) The LVF 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.

Emergency Call Routing Function (ECRF) - 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.

Legacy Network Gateway (LNG) - 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, may be provided by the State, or may be provided by a PSAP, in any combination as desired and required.

1.1.3 Egress to Public Safety Answering Points and Regional Emergency Services IP Networks

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 perform the inverse function of an LNG, to convert the NENA i3 format back to legacy formats. The main concern 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 balance of this page is intentionally left blank.

3. STATEWIDE EMERGENCY SERVICES IP NETWORK REQUIREMENTS AND SPECIFICATIONS

It is understood that as a possible Statewide ESInet provider, OARnet offers service level objectives. These are similar in nature to quality of service agreements. Standards for network services to establish and maintain an emergency services quality network that is available 99.999 percent in both quality and availability are provided by NENA.

However, it is recognized that not all locations currently have access to OARnet. It is necessary for Ohio to set the requirements and specification for the Statewide ESInet regardless of the network provider or providers.

The following ESInet technical requirements reference the industry best practices per NENA i3 standards for the requirements and specifications for an ESInet.

3.1 Emergency Services IP Network Requirements

The network begins with physical facilities which provide the actual transport of IP packets. Typically these are considered OSI layers 1, 2, and 3.

Per NENA 08-003 an ESInet is defined as follows:

An ESInet is a managed IP network that is used for emergency services communications, and which can be shared by all Public Safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core functional processes can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based inter-network (network of networks).

ESInets designated to transport emergency calls should satisfy these requirements:

- Be a private or virtual private network (VPN) based upon Transmission Control Protocol (TCP)/IP
- Provide scalable bandwidth to support new and enhanced services
- Provide a conventional routed IP network
- May utilize Multiprotocol Label Switching (MPLS) or other sub-IP mechanisms as needed
- Utilize redundancy to obtain high availability and reliability
- Be resilient, secure, physically diverse and logically separate from other IP networks
- Be engineered to sustain real time traffic, including data, audio and video
- Support secured TCP connections
- Be capable of operating on both IPv4 and IPv6 protocols

3.1.1 Next Generation 9-1-1 Network Backbone

The requirements in this section are designed to ensure the suitability of the network for the purpose of transporting NG9-1-1 services and other Public Safety applications. The proposed ESInet infrastructure shall be an open-standards-based, private, secure, extensible and highly available IP network.

These requirements are drawn from the State's perspective, and therefore may not specify each and every element necessary for a vendor to deliver the NG9-1-1 services as specified herein. Should the State decide to move forward with a request for information (RFI) or request for proposal (RFP), a vendor, as the expert, is expected to design, propose and implement the

most effective and efficient solution at the most cost effective price. The ESInet must be capable of supporting NG9-1-1 core functions to be deployed state-wide. These functions include but are not limited to the following:

- Border control function (BCF)
- Policy routing function (PRF)
- Emergency services routing proxy (ESRP)
- Legacy network gateway (LNG)
- Emergency call routing function (ECRF)

A NG9-1-1 services provider will provide all of the above NG9-1-1 core functions, except ECRF functionality. The NG9-1-1 services provider shall provide a solution that exclusively utilizes the Internet Engineering Task Force (IETF) LoST protocol (RFC-5222) to interface the ECRF with the rest of the NG9-1-1 solution such that external RFC-5222-compliant ECRFs may be used in place of Respondent-supplied ECRF(s).

The ECRF in Ohio will be a part of a (possibly separate) GIS Services contract. Because the GIS Services vendor will provide, as part of this contract, the ECRF features then the vendor(s) who would respond to a RFI or RFP for NG9-1-1 services will not be required to provide an ECRF. Instead, the ESInet vendor must provide co-location services to the GIS vendor for the GIS vendor's ECRF solution, or ESInet IP connectivity to at least two Points of Presence (POPs) (as required by the GIS vendor) for the purpose of establishing ECRF connectivity. The ESInet vendor will provide IP addresses and other information as required to interconnect the external ECRF to ESInet and/or NG9-1-1 services that are the subject of these specifications.

In the case of a RFI or RFP, vendors should be encouraged to provide information regarding improvements or alternatives to these requirements in their response. Unless otherwise agreed to during a RFP process, the proposed IP network shall satisfy the characteristics and performance specifications as stated in this section.

3.1.1.1 General Requirements

3.1.1.1.1 Federal Communications Commission Rules

All equipment must conform to Federal Communications Commission (FCC) Rules Part 15, Class A (commercial, non-residential radiation and conduction limits) for electromagnetic interference (EMI).

3.1.1.1.2 Industry Standards

Where applicable, all equipment must comply with applicable industry standards, such as:

- Underwriters Laboratories (UL)
- International Organization of Standards (ISO)
- Open System Interconnection (OSI)
- Institute of Electrical and Electronics Engineers (IEEE)
- American National Standards Institute (ANSI)
- Electronic Industries Alliance (EIA)

- Telecommunications Industry Association (TIA), (including American National Standards Institute (ANSI)/EIA/TIA-568 Commercial Building Telecommunications Wiring Standards), etc.
- Equipment shall be compliant with NENA i3 standards.

3.1.1.1.3 Facilitating Carrier Transition

The vendor shall be responsible for the migration of existing 9-1-1 services to the ESInet and to NG9-1-1 services at all interfaces between the vendor and other emergency call originating network operators in order to accomplish 9-1-1 call delivery which meets the quality and reliability requirements. This includes stating the terms, conditions, procedures or processes for interconnection and exchange of information between other carrier's networks and systems and the vendor's networks and systems. Unless the parties otherwise agree, such terms, conditions, procedures or processes shall follow applicable Ohio Public Utilities Commission telephone industry practices, NENA standards and recommended practices, or applicable US telecommunication law. The terms, conditions, procedures or processes shall not impose onerous requirements on other network operators, and shall be stated in any proposed solution. Examples of such interfaces would be the means to perform the timely exchange of information such as legacy Automatic Location Identification (ALI) database updates, exchange of monitoring/trouble ticket statuses, trunk connections to the LNG and IP connections to border control functions. This list of examples is not exhaustive. The vendor is expected to work closely with other network operators and to cooperate fully with them in order to accomplish successful transition to the NG9-1-1 call delivery system.

The ESInet will be capable of servicing all PSAP CPE from NG9-1-1 i3 compliant systems to legacy 9-1-1 ANI/ALI controllers via LPGs.

3.1.1.2 Emergency Services Internet Protocol Network Requirements

3.1.1.2.1 Open Standards Based

The proposed emergency services network shall be open standards based. The vendor shall specifically identify if any portion of the solution which is considered proprietary.

3.1.1.3 Quality of Service Features

The network shall have quality of service (QoS) features suitable for the real-time transport of VoIP traffic requesting emergency services. The network shall support voice quality objectives equivalent to an ITU-T G.800 Mean Opinion Score (MOS) of 3.8 at least 99 percent of the time, and a mean opinion score (MOS) score equivalent of 2.5 at least 99.9 percent of the time.

3.1.1.4 Emergency Services IP Network Suitability

The proposed ESInet shall be suitable for transporting emergency calls and associated data for all NG9-1-1 applications.

3.1.1.5 Emergency Services IP Network Interconnections

The ESInet shall interconnect all End Sites and data centers. An End Site is any PSAP site, first responder site, authority office site, or any site that is directly connected to the ESInet. The State may, at its option and discretion, choose to deploy more or fewer End Sites. End Site additions or eliminations may result in reallocation of the total emergency call traffic volume and total Core Network bandwidth among the remaining sites.

Such reallocation, if any, may require adjustments to the number of answering positions and site access network bandwidth among the remaining sites. Because of these considerations, pricing must be itemized by each End Site.

3.1.1.6 Bandwidth Growth

The proposed ESInet shall be able to accommodate growth of bandwidth, interconnection to additional End Sites, in Ohio and interconnection to other national and/or state-level ESInets in the future.

The proposed ESInet shall support such future growth and interconnections with minimum impact on the proposed infrastructure through incremental additions to the existing network.

3.1.1.7 Real Time Monitoring

The proposed IP network shall be monitored in real time for the satisfactory operation and security of all significant components and required performance parameters.

The State or its designated representative shall be able to ascertain the status of major IP network elements by viewing a status map or display with a Web browser which is connected to the ESInet, or via a similar tool or mechanism.

3.1.1.8 ESInet Architecture Overview

The State does not prescribe how the vendor shall implement the IP network. The State's view of the ESInet is at OSI Layer-3, that is, the delivery of IP packets between nodes on the network. From the State's perspective, and in the absence of specific security policies as specified by State, the network shall deliver IP packets from any IP address to any other IP address among any and all connected End Sites.

Vendors may select any Layer-1 (copper, fiber, wireless, etc.) and any Layer-2 (High-Level Data Link Control [HDLC], frame-relay, Asynchronous Transfer Mode [ATM], MPLS, etc.) technologies, in any combination and arrangement that will deliver the most cost effective solution that satisfies the requirements.

3.1.1.9 Provision of Layer-1/Layer-2 Facilities

Vendors shall provide, directly or through subcontractors, the Layer-1/Layer-2 facilities, as may be required, to interconnect to the specified End Sites.

3.1.1.9.1 Layers 1 and 2

Vendors shall 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.

3.1.1.9.2 Network Diagram Clarity

Network diagrams shall display enough information about the core network and about each unique type of End Site connection so that the topology and design, and the selection of the Layer-1, 2, and 3 technologies are clear.

3.1.1.9.3 Network Diagram and Narrative Information

Network diagrams and narrative shall provide sufficient information so technical reviewers can identify how the design meets the requirements and intent of this document. The drawings, narrative or tables shall convey all points of interconnection (POIs) and/or hub locations.

3.1.1.10 Layer-3

In normal (all up) operation of the ESInet, the Layer-3 IP service shall meet the service level requirements.

3.1.1.10.1 No Single Point of Failure

Except for PSAPs identified as non-redundant (sites with three or fewer seats), the failure of any single ESInet component shall not interrupt the delivery of IP traffic between interconnection points, delivery of IP traffic to redundantly connected End Sites, or to maintain the operation of network services such as network monitoring services.

3.1.1.10.2 Open Standards

The proposed network shall 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 the applicable Request for Comments (RFCs), at ISO Layer-3 and above.

3.1.1.11 Blocking or Inhibition of Protocols

All standard protocols that use IP for transmission shall be transported over the proposed network. No specific protocol or use of the IP network may be blocked or inhibited by the ESInet provider, except to comply with State-specified security policies.

3.1.1.12 Proprietary Standards

Vendors shall reveal any use of proprietary standards or protocols in their proposed solution or state that they fully comply with the open standards requirement. Any limitations, whether technological or policy related, shall be revealed.

3.1.1.13 Scalability – Expansion Requirements

The overall design shall scale with respect to bandwidth, additional sites and interconnection with other ESInets. The design shall permit a doubling of bandwidth, the doubling of the number of connected sites, and/or interconnections to as many as five additional 9-1-1 call delivery ESInets such as ESInets in adjacent states.

The design shall accommodate this level of expansion without wholesale replacement of network components, fork lift upgrades of Core components, or excessive non-incremental costs. For example, if doubling the bandwidth requires replacement of all Core network routers, then this requirement has been violated. However, if the addition of a site requires installation of additional interface cards and site-specific routers, or even the addition of a Core router that can be shared among several additional sites, then this will be considered normal incremental cost, and this requirement will still be satisfied.

3.1.1.14 Diagrams and Narratives

Vendors shall demonstrate, through the diagrams, narrative and pricing, how this goal can be realized within the proposed network design. This narrative shall explain changes or upgrades to proposed components of the network that would be required to accomplish this level of expansion.

3.1.1.14.1 Architectural Survivability

The Core Network and the redundantly connected sites shall 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.

3.1.1.14.2 Network Diversity

The proposed network shall incorporate service provider and/or facility/media diversity wherever it is economically reasonable to do so. The vendor shall identify cost estimates for complete diversity.

3.1.1.14.3 Diversity Requirements

Where economically available, the network Core solution and redundantly connected End Sites shall include physically diverse routes and physically diverse building entrances. The vendor shall identify cost estimates for complete diversity.

3.1.1.14.4 Non-Diverse Network Elements

Any network elements that are not provisioned with physical diversity shall be disclosed and explained in the proposal.

3.1.1.15 Network Availability

Assuming full redundancy has been implemented at all End Sites and ignoring possible diversity limitations, the proposed network shall be designed to provide 99.999 percent availability to all sites as measured monthly. Vendors may be required to defend their claim of a 99.999 percent design by producing statistics on mean-time-between-failures and other data on critical network elements together with a risk analysis.

3.1.1.16 Redundancy Threshold

The vendor shall price the solution on a per workstation basis, and PSAPs below the threshold of three or fewer workstations shall not require full network redundancy.

3.1.1.17 Response Times

Twenty-four hour technical and maintenance support shall be available with a response time, on site, of no more than two (2) hours for major failures. This support shall be available 7x24x365. A complete listing of all warranties including systems and equipment, detailing what is included and what is not included shall be provided. The vendor shall specify the number of trained technicians locally available.

3.1.1.18 Quality of Service

There are QoS performance requirements related to the network that must be maintained. The following network performance requirements are taken directly from NENA 08-506, Version 1, December 14, 2011:

➤ **Packet Loss**

An overall (end-to-end) packet loss budget for maintaining intelligible voice transmission is about 5 percent. Out of that 5 percent budget approximately one half of the packet loss should be allocated for the ESInets with the remaining allocated for the origination network. It is a best practice to engineer ESInets to keep the packet loss budget under 2.5 percent. ESInets should be designed without oversubscription.

The State of Ohio requires packet loss of less than 1 percent shall be achievable on such ESInets.

➤ **Jitter**

It is a best practice to design ESInets to maintain less than 20mS variation in the end point jitter buffers.

➤ **Latency**

The one-way transit delay (i.e. end-to-end, mouth to ear) for real-time media packets should not exceed 150mS. (ITU-TG.114). The maximum acceptable delay for packets traversing the ESInet should be less than or equal to 35mS. This allows the original encode and decode and a conference bridge in the middle of the path and still achieve the maximum 35mS or less packet delay.

The State of Ohio requires design of the ESInet to operate with less than 20mS of latency.

3.1.1.19 Network Upgrades and Maintenance

The proposed Core network and redundantly connected End Sites shall not be adversely impacted by down time for planned maintenance. It is acceptable that individual components or elements have down time for planned maintenance.

3.1.1.19.1 Down Time Disclosures

Vendors shall, five business days in advance, disclose any service impact, limitation or operational issue that may arise as a consequence of planned or immediately prior to unplanned down time of any such individual component.

3.1.1.19.2 Planned Maintenance

Planned maintenance shall be performed in accordance with an appropriate standard operating procedure (SOP) designed to mitigate the operational impact of such maintenance. Scheduled downtime must be coordinated with the State with at least five business days advance notice prior to performing the scheduled downtime in order for the downtime not to be calculated into the monthly network availability factor.

3.1.1.19.3 Standard Operating Procedure Availability

Standard operating procedures shall be made available to the State upon request.

3.1.1.20 Bandwidth

The vendor shall state their bandwidth requirement for the NG9-1-1 call delivery system for one PSAP workstation, assuming a voice call in progress meeting the voice quality requirements of this document. If this value exceeds 300 kilobits/second, the vendor must justify the requirement by providing the rationale and/or basis for the bandwidth calculation.

The bandwidth requirements are for a fully functioning network with all 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 in the event of a failure or a scheduled maintenance activity.

3.1.1.20.1 Calculation of Bandwidth

The vendor shall calculate the minimum bandwidth required between the Core network and any End Site (the access network) by multiplying by the total number of workstations at that site by the requirement per workstations as stated above, and then add at least 50 percent to that sum.

3.1.1.20.2 Minimum Bandwidth

If the expected bandwidth is calculated to be less than 1.5 megabit/second, then the minimum bandwidth to any End Site shall be 1.5 megabit/second.

3.1.1.20.3 Bandwidth Expansion

The proposed solution shall support a growth in bandwidth at each End Site to at least double the initial requirements by adding facilities or using faster facilities, but without replacing major components such as Core or on-site routers.

The network must be built to 100% expansion capability. Once capacity on the network hits 60% utilization, bandwidth planning must be initiated, and bandwidth allocation shall be increased before the utilization reaches 80% for more than 5% of the time measured on 5 minute intervals.

3.1.1.21 Network Facilities

Access network facilities that connect an End Site, such as a PSAP site, to the Core network, meet the Core network at a POI (A POI could be another PSAP site). The Core network (POI-to-POI connections) shall be able to sustain IP traffic without

limitations assuming all End Site interconnections, as discussed in the previous section, are operating at full bandwidth capabilities.

3.1.1.21.1 Access Network - End Site Interface

At each redundant End Site, the access network to End Site demarcation interface to the site's local area networks (LANs) shall be two redundant 100-megabit or faster unshielded twisted pair (UTP) Ethernet ports. The NG9-1-1 services component of this document may require the vendor to provision LAN(s) at the site. Such LANs are not considered to be part of the core network or access network, but are a component of the complete ESInet infrastructure.

3.1.1.21.2 No-Single-Point-Of-Failure Requirement Compliance

In order to comply with the no single-point-of-failure requirement, the two demarcation Ethernet ports shall not be provisioned on the same piece of hardware, such as a single Ethernet switch or router. Non-redundant sites may utilize a single 100-megabit or faster UTP Ethernet port.

3.1.1.21.3 Ethernet Failover

For redundant sites, the vendor shall list and describe the Ethernet port fail-over scheme. The fail-over scheme shall be one that is widely used in the industry and that complies with open standards.

3.1.1.22 Internet Protocol Addressing

The proposed IP network infrastructure shall support and route both an IP version 4 (IPv4) address space and an IP version 6 (IPv6) address space as two "virtual" but independent networks. Alternatively, the IPv4 network may be encapsulated in the IPv6 core and access networks, with encapsulation occurring at the access network side of the End Site demarcation interface. The use of encapsulation does not relieve the vendor from being able to monitor the operation of the IPv4 network as required in the RFI or RFP.

At the State's request and discretion, the vendor may be requested to provision an additional (third) IP address space, as a logically separate IP network, for example as a VPN or encapsulated network. The purpose of this third logical IP network would be to securely separate other Public Safety applications and interconnections from the NG9-1-1 call delivery application.

3.1.1.22.1 Internet Protocol Version 6 Address Space

The vendor shall obtain/provide an IPv6/48 allocation for the ESInet.

3.1.1.22.2 Emergency Services IP Network Allocation

The IPv6 allocation shall be announced by at least two routers in the Core Network.

3.1.1.22.3 Internet Protocol Version 6/64 Block Assignment

The vendor shall assign one IPv6 /64 block to each site as a subnet of the /48 announcement.

3.1.1.22.4 Subnet Number Assignments

The subnet number for each site assigned prior to deployment shall be reported to the State.

3.1.1.22.5 Core Network Provisioning

The core network, including links to routers located at the sites, shall be provisioned with IPv6 addresses from the announced/48 block.

3.1.1.22.6 Network Static Addressing

The proposed network shall be statically addressed at all major network interfaces, such as router interfaces.

3.1.1.22.7 “Loopback” Interface

A “loopback” interface with a static IPv6 address shall be assigned to each network element that is capable of IP administration, such as a router, switch or server.

3.1.1.22.8 Conducting Network Monitoring

To the maximum extent possible, network monitoring and administrative functions shall be conducted via the IPv6 network. Vendors shall highlight their IPv6 capabilities.

3.1.1.22.9 Internet Protocol Version 4 Address Space

Vendors shall assign either at minimum one-half of a public Class B (/17 allocation) for the use of the Ohio ESInet, or if unavailable private IPv4 addresses from the 10.39.0.0/16 address space. Public IPv4 addresses are much preferred.

3.1.1.22.10 PSAP Site Address Allocation

Each PSAP site shall be assigned an IPv4 address block with a minimum of 12 + number of answering positions host addresses. So, for example, a two position PSAP would require a /28 allocation, while a larger PSAP would require a /27 allocation.

3.1.1.22.11 Subnet Number Assignments

The subnet number for each site shall be reported to the State.

3.1.1.22.12 Internet Protocol Version 4 Connectivity

The IPv4 connectivity shall be established between each site, either by native IP routing or by tunneling through the IPv6 network, at the vendor's option.

3.1.1.22.13 Internet Protocol Version 4 Specific Functions

Vendors shall list network functions, such as monitoring or administrative functions, that they can only perform using IPv4. The successful vendor may be required to work with entities that presently implement only IPv4 addresses to assign a suitable IPv4 address to their Ethernet demarcation connection and to tunnel or route IPv4 addresses outside the public class B block or the private 10.39.0.0 block through the network to other sites, as needed.

3.1.1.22.14 Entity Cooperation

While the vendor shall not be required to make changes in entity IP networks that are outside the scope of this document, the vendor shall be required to fully cooperate with those entities. For example, the vendor shall provide information, perform configuration changes in edge network routers, to change entries in core domain name system (DNS) services, and, in general, assist entities in utilizing the ESInet to the fullest extent possible while in compliance with State policy.

3.1.1.23 Internet Protocol Routing

The Core IP network shall implement a dynamic IP routing protocol. The State 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 consideration, provided the solution is open standards-based and is supported on Linux, Microsoft and Unix hosts.

3.1.1.23.1 Internet Protocol Packet Delivery

The IP routing protocol shall provide for the delivery of IP packets from any IP address to any other IP address within an address space in the ESInet, or to any connected IP network, or to reachable IP networks via a connected IP network.

3.1.1.23.2 IP Routing Problem Resolution

The selected vendor shall work with the operators of interconnected IP networks to resolve IP routing problems as a feature of the supplied service.

3.1.1.23.3 Automatic Internet Protocol Rerouting

The IP routing protocol shall be set up to provide automatic IP rerouting in the event of a failure of any network facility or component, even if automatic rerouting is provided at another OSI Layer, such as Layer-2.

3.1.1.23.4 Network Stability

The dynamic routing protocol shall be configured (tuned) to mitigate IP route instability in the network.

3.1.1.23.5 Loss of Bandwidth

The dynamic routing protocol shall be configured 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.

3.1.1.23.6 Internet Protocol Routing Protocol Implementation Narrative

The vendor shall provide a short narrative describing the IP routing protocol implementation. This narrative shall describe how the network responds to various failure scenarios and how route instability in the network is avoided.

3.1.1.24 Quality of Service

The proposed network shall implement a QoS function that can assure timely delivery of Real-time Transport Protocol (RTP) packets even in the presence of network congestion from other non-real-time protocols, up to the limit of the available bandwidth. A differentiated services (DiffServ) QoS scheme is requested.

3.1.1.24.1 Non-Real Time Traffic Prioritization

The QoS system shall also be able to prioritize other non-real time traffic, such as Session Initiation Protocol (SIP), if needed.

3.1.1.24.2 Real-time Transport Protocol Streams

Quality of Service support for RTP streams shall be configured into the network. The design shall minimize excessive latency and jitter.

3.1.1.24.3 Bandwidth Sharing

The proposed QoS or IP routing scheme shall ensure that a specific RTP session does not “share” bandwidth on redundant links. This requirement is to ensure that RTP packets in user datagram protocol (UDP) streams do not arrive at the destination out-of-sequence should the redundant links have considerably different latencies.

3.1.1.24.4 Traffic Prioritization Narrative

Vendors shall provide a brief narrative overview of how they prioritize traffic across the network. Any interaction between the QoS implementation, IP routing or other protocols shall be revealed and explained.

3.1.1.25 Network Address Translation

The use of Network Address Translation (NAT) within the proposed IP network is highly discouraged and is prohibited within both the IPv6 and the IPv4 10.39.0.0 address spaces. Network Address Translation presents special problems for the reliable implementation of SIP and RTP streams that traverse the NAT device. Vendors that use NAT shall demonstrate their understanding of the SIP/RTP/NAT problem and explain how they intend to mitigate any issues that might arise.

3.1.1.26 Back-to-Back User Agent Usage

Network Address Translation capability at points of interconnection with other IPv4 networks/address spaces may be required in order to resolve possible IPv4 addressing issues. However, if SIP or RTP traffic needs to cross such boundaries, it shall be handled with back-to-back user agent (B2BUA) type of session border controllers (SBCs), rather than via NAT. Back-to-Back User Agents shall also be used to transport SIP and RTP between IPv6 and IPv4 networks, if required. If required by the application, the session boarder control (SBC) shall be able to forward SIP location conveyance data between the User Agents (UAs).

3.1.1.27 Network Monitoring

The ESInet transport infrastructure shall be monitored on a 24x7x365 basis.

3.1.1.27.1 Simple Network Management Protocol Version3 Support

All IP manageable network hardware shall support the Simple Network Management Protocol version 3 (SNMPv3) specification for performance monitoring via standard management information base (MIB) objects.

3.1.1.27.2 Network Fault Monitoring

Fault monitoring shall detect and log IP network problems, notify the network operator, and depending on severity and policy, provide timely notification of designated State staff. Examples of such network problems include failed circuits, equipment or network functions. If the failure is transitory or immediately corrected, notification is not required, but all events shall be logged and included on required reports. All system alarms are required to be monitored in the call-taking/dispatch area of the PSAP. An externally-mounted alert system is required to indicate a failure. All audible alarms will be able to be silenced until the event is cleared.

3.1.1.27.3 Network Performance Monitoring

Performance monitoring shall measure the variables that affect network performance.

3.1.1.27.4 Information Retrieval

Vendors shall describe how their monitoring solution stores information for reporting and subsequent retrieval purposes, including any requirements for accessing such features by the State.

3.1.1.27.5 Network Operations Center

The vendor shall utilize a Network Operations Center (NOC) which is staffed to support 24x7 restoral or mitigation of incidents. The NOC must have a disaster recovery plan that is tested regularly.

3.1.1.27.6 Trouble Ticket System

The vendor shall have a 24x7x365 trouble ticket system. The vendor shall describe the system's capabilities and procedures involved in generating, resolving and reporting on trouble tickets for all (network, PSAP, training, reports, etc.) problems. In addition to supplying a 24x7 toll free number, the vendor shall also describe other methods of generating (email, text msg., etc.) and acknowledging trouble tickets.

3.1.1.28 Managed Network Services

The Vendor shall supply and describe their Managed Network Services (MNS) system, including, but not limited to:

- Operating system updates
- Anti-virus software
- Security software
- Applications software
- Disaster recovery
- MNS services that are out-sourced
- State access to view system status

3.1.1.28.1 Vendor Contact Number

The vendor shall provide a 24x7x365 toll free number accessible to authorized personnel, as determined and authorized by the State.

The use of the network monitoring system does not preclude the State 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 for other such applications.

3.1.1.28.2 Standards

Vendors shall have general knowledge of IP network security systems, and the standards found in these documents:

- NENA NG-SEC Document 75-001
- NENA i3 Technical Requirements Document 08-751
- NENA Detailed Functional and Interface Standards for NENA (i3) Solution Stage 3 08-003

Security in the ESInet shall be in accordance with the requirements below and any security policy as approved by the State. The State may modify the security policy at any time at its sole discretion.

3.1.1.28.3 Access Control

The vendor's security management solution shall control access to network resources according to Public Safety network security guidelines to prevent sabotage and the compromise (intentional or unintentional) of sensitive information.

3.1.1.28.4 User Monitoring

Security management shall use Public Safety network security standards to monitor users logging into the network resources and refuse access to those who enter inappropriate access codes.

3.1.1.28.5 Security Techniques and Protocols

The proposed network shall support standard security practices that may include the use of anti-virus software, virtual local area networks (VLANs), VPNs and secure sockets layer protocols.

3.1.1.28.6 Interconnection of Other Networks

The ESInet may be used to interconnect other edge site LANs or VLANs, not part of the NG9-1-1 call delivery system, across the state of Ohio. These LANs/VLANs may interconnect computer aided dispatch (CAD) systems and other Public Safety applications as approved by the State. Such interconnection must be accomplished using a logically separate (third) IP address and routing space, VPNs, tunnels or other mechanism to keep the IP traffic separated from the NG9-1-1 call delivery system.

3.1.1.28.7 Logically Separated Next Generation 9-1-1 Local Area Networks

Any LAN(s) supplied and installed at a PSAP or other EndSite to provide NG9-1-1 call delivery services, as required as part of this document, is intended to be a limited access and secure LAN(s) or VLANs. Call delivery LANs or VLANs shall not be interconnected with any other LAN(s) at the PSAP/edge site, and shall run in the NG9-1-1 call delivery system address space. However, End Sites may interconnect other LANs or VLANs to the ESInet to supporting CAD or other public safety

applications, provided such LANs or VLANs operate in separate IP address and routing domains as specified elsewhere in these requirements.

3.1.1.28.8 Physical Port Protection

Any empty, spare or otherwise unused Ethernet ports on equipment (such as routers and switches) supplied as part of this document which are part of the call delivery IP address space shall be administratively disabled at the time of ESInet and NG9-1-1 service is commissioned. Protection Against User-Loaded Software

3.1.1.28.9 Protection Against User-Loaded Software

Any workstations or computer equipment which provide emergency call delivery functions, if equipped with Universal Serial Bus (USB) ports and/or removable media storage devices, shall have such USB ports and/or removable media storage devices physically or administratively disabled or otherwise restricted, such that jump drives or removable media cannot be readily used by casual users to upload executable software into the workstation or equipment without access to administrative accounts, or modification of the equipment.

3.1.1.28.10 Other Network Qualification

Any IP network that connects to the ESInet shall be required to comply with standards, including the security standards, and demonstrate compliance through an initial and recurring audit.

3.1.1.28.11 Anti-virus Software

Vendors shall provision one anti-virus firewall or gateway at each edge site to support safe and secure interconnection of non-NG9-1-1 LANs across the State.

3.1.1.28.12 Anti-virus Database

The anti-virus firewall shall use an antivirus database to scan incoming and outgoing packets for the presences of malicious software, and block and log such activities. The vendor shall describe how they will maintain the anti-virus database.

3.1.1.28.13 Security Logging

Security events, including failed logins, antivirus updates, antivirus detection and other security events must be logged. The vendor shall describe how they will monitor and log the ESInet for security violations, and what activities will be logged.

3.1.1.29 Transient Voltage Surge Suppression

In addition to primary protection, secondary Transient Voltage Surge Suppression (TVSS) shall be installed.

3.1.1.29.1 Copper Pairs

All copper pairs entering the building shall be provided with secondary Transient Voltage Surge Suppression (TVSS) protection.

3.1.1.29.2 Transient Voltage Surge Suppression Device Protection

Transient Voltage Surge Suppression devices shall protect all incoming and outgoing equipped ports that are or could be connected to wireline or wireless facilities. These facilities include central office (CO) plain old telephone service (POTS), 9-1-1 trunks, T1/DS1 facilities or State owned customer premise equipment (CPE) and facilities.

3.1.1.29.3 Installation Kit

The vendor shall include an installation kit including all ground bars and ground wiring for installation at each site for the vendor's equipment. Vendors may assume a suitable ground exists. If it does not exist, a suitable ground shall be provided at the State's expense.

3.1.1.29.4 Clamping Voltage

The secondary TVSS devices shall list a clamping voltage of 250 volts (.5kV) or less and operate in <10 nanoseconds.

3.1.1.29.5 Underwriter Laboratory 497A Requirements

The device shall meet Underwriter Laboratory (UL) 497A requirements and shall have an operational indicator to alert maintenance personnel that the device has been utilized, failed or that the circuit is unprotected.

3.1.1.29.6 Audio Signaling Degradation

The secondary TVSS shall not degrade the audio signaling.

3.1.1.29.7 Manufacturer's Warranty

The secondary TVSS shall have a minimum of a one year manufacturer's warranty.

3.1.1.30 Spares

Vendors shall describe their spares program including stocking levels and locations and the time required for an on-site field technician to access a spare. The role of State, if any, in spare stocking or access shall be explained.

3.1.1.31 Current and New Equipment

Only new equipment shall be considered. Refurbished or used equipment shall not be considered as part of the proposed solution.

3.1.1.31.1 Hardware Age and Support

The State requires that proposed hardware be of current manufacture and fully supported.

3.1.1.31.2 End of Maintenance/Support Equipment

Equipment that has been announced as end-of-sale within one year of installation is not acceptable.

3.1.1.31.3 Use of End-of-Sale Equipment

If a proposed device or software goes into end-of-maintenance/support status within the contract period, its equivalent or better current manufacture shall be installed at the vendor's expense unless agreed otherwise.

3.1.1.32 Inactive Connections

As not to incur costs for inactive network connectivity, the successful vendor is expected to collaborate with the State to develop a plan to utilize network connections in a phased approach as PSAPs are migrated to the Statewide ESInet.

3.2 Emergency Services IP Network Operational Specifications

In addition to ESInet technical requirements outlined in Section 3.1 of this document, the State of Ohio also seeks to outline operational requirements that are important for the network to operate at a level that meets the needs and expectation of the state and the PSAPs across the state. The ESInet vendor should provide operational information to the State as part of their contract. The operations information should include, at minimum, the following:

- Mission Statement
- Types of Services
- Optional Services
- Operational Activities
- Change Management
- Configuration Management
- Data Management
- Trouble Management Support
- Escalation Procedures
- Major Outage Process
- Testing Disaster Recovery Solutions with the NOC
- Ordering NG-911 Routing Services
- Billing
- NG-911 Network Management System (NMS) Tools
- NG-911 System Engineering and Design
- NG-911 MIS tools
- Security
- Staffing
- Hours of Operation

Additionally, the ESInet backbone vendor will be required to manage the network and provide specifications for quality management to include:

- IP Addressing
- Dynamic Routing Protocols
- Availability and Reliability
- Network Security

- Network Management and Monitoring
- Performance Requirements
- Hardware Network Elements
- Service Level Objectives

3.2.1 Managed Network Services

3.2.1.1 Operations Requirements and Assumptions

The vendor shall provide managed services and be required to establish or demonstrate practices and procedures for performing its functions on behalf of the State. The vendor will be required to track its activities utilizing a suitable tracking system that will preserve and document all activities. These activities include but not limited to:

- Hardware Network Elements
- Network Management
- Capacity Management
- Change Management
- Configuration Management
- Implementation Management

The vendor will be the single point of contact for change management for emergency services call and information delivery in the State. They will provide these services 7x24x365. They will provide staffing to meet these requirements listed below:

1. Oversight of the ESI-net (application layer) service
2. Oversight of the IP network (layer 3 and 4 services)
3. State-provided and State-hosted PSAP solutions down to call-taker workstations

The requirements related to these oversight functions are outlined below.

Oversight of the ESI-net network service

- A. Maintain a database of service providers to include,
 - a. Contact information
 - b. Type of connection
 - c. Network interconnection points
 - d. Technical specifications and configurations such as trunk counts, types and signaling formats
 - e. Other data as specified by the State.
- B. Maintain a database of PSAPs that includes
 - a. Contact information
 - b. Equipment type, brand, model and configuration
 - c. PSAP vendors used and equipment and services provided by vendor
 - d. PSAP IP addresses
 - e. Technical specifications of equipment, such as number of ports and signaling formats
 - f. For SIP capable PSAPs
 - i. SIP Uniform Resource Identifiers (URI) for 9-1-1 calls
 - ii. SIP location conveyance capabilities
 - iii. Media capabilities (voice, video, text)
 - iv. Available codecs
 - v. SIP conferencing and transfer capabilities
- C. Maintain a database of PSAP vendors that includes

- a. Contact information
- b. Emergency problem resolution procedures
- D. Develop and regularly update a statewide deployment plan, including
 - a. PSAP identification
 - b. PSAP jurisdiction
 - c. Service provider identification
 - d. Service provider operating area
 - e. PSAP and service provider deployment schedules.
- E. Develop or demonstrate a Change Management Process and will implement the change management process. The principles are that any change must be authorized, must have been carefully considered and planned, must be made in such a way that it does not endanger the operation of the service, that all affected parties that are or might be effected are identified and are properly informed, and that a workable plan and schedule for implementation has been developed.

It should be noted that some changes may be relatively simple to review, plan, and implement (such as changing a destination in an existing call overflow plan) while other changes may be very complex and potentially disruptive (such as a PSAP relocation). The Change Management process developed must be able to accommodate both simple and complex changes with the required cost and effort in scale with the complexity of the change, even while protecting the integrity of the service and fidelity to the policies of the State.

The satisfactory change management process will include, but not necessarily limited to, the following.

- a. A process for making a change or reconfiguration request. The change or reconfiguration request may originate from any stakeholder, and must be accompanied with enough information that the vendor can determine that the request can satisfy the requirements of the change process. The vendor is responsible for communicating the requirements for the change request to the requestor. If, in the review process, a change request cannot satisfy the requirements of the change process it may be returned to the originator be possibly be modified and resubmitted, or rejected. If a change request is not accepted, the vendor must provide the requestor with an explanation of the reason for the rejection, or with information on how the request might be modified so that it can be accepted. All change requests will be recorded and their disposition documented.
- b. The vendor (or a change review officer, committee or board) must review a change request. Impacts to the network such as time, activity sequence, scheduling and cost will be carefully analyzed and the final decision will be made in accordance to approved guidelines. The review must include consideration of these items:
 - i. Authorization – is the requestor authorized to make requested change
 - ii. Clarity – is the purpose or goal of the change sufficiently clear to implement
 - iii. Compliance – is the change compatible with the policies and goals of the State
 - iv. Feasibility – is the change technically sound and can it be safely implemented without danger to the 9-1-1 service
 - v. Identification – All parties that will be affected by the change, or who require knowledge of the change, must be identified.
 - vi. Procedure – is there a standard method of implementation
 - vii. Recovery – if the change causes an unexpected problem is there a safe back-out/restoration procedure
 - viii. Resources – what resources are required to implement the change
 - ix. Security – are there security implications
 - x. Side effects – what impacts will the change have on apparently unrelated functions

- xi. Test plan – what post change functions need to be verified

The review process will be recorded and documented. If a change request satisfies the review and is documented it is ready for scheduling and implementation

- c. The vendor will schedule implementation of a change that completes the review process. A schedule is set up and all identified entities will be notified. Log entries will be made to record the actual work performed and time and date of the work, and the results of the test plan. If unexpected problems or results are encountered, the recovery procedure is invoked and documented and the change is returned for additional review.
- d. At the completion of a change the vendor will update all documents and records in the management system as required by the change

The vendor must publish its change management procedures and make this information available to the State and to stakeholders.

- F. Service provider business relation management:
 - a. The vendor will be the primary contact for all service providers. All connections (data/voice) into the system will be coordinated through the Vendor.
 - b. The vendor will document all data from service providers.
 - c. The vendor will write all State 9-1-1 service provider orders.
- G. The vendor will develop and implement a process for ALI Database Management, and will maintain its own instance of these databases. The database management process must observe and implement NENA technical and operational standards. The ALI information must include the actual ALI records, or, for pANI records, the ALI service provider NENA code which could be used to steer an ALI request to the appropriate ALI service provider. The vendor will execute intercompany agreements with all service providers in order to obtain and process this data in a timely fashion and in compliance with NENA operational standards.
- H. Alternate and overflow routing
 - a. The Vendor will develop a call overflow scheme with each PSAP in the state.
 - b. The Vendor will document and test all call overflow/alternate routing configurations.
- I. Call logging/stats reporting
 - a. The service provider will provide the vendor on-line access to call traffic logs
 - b. The vendor will report summaries and findings to the State quarterly, or as requested by the State
 - c. Web based tracking and reporting tools are highly recommended. To include trouble ticket initiation, trouble history tracking and resolution status.
- K. Monitoring and Orders
 - a. The service provider has established customary and reasonable order processes so that the vendor can place orders.
 - b. The vendor will require an IP connection to the 9-1-1 over the network for monitoring, access to databases and logs and for initiating test calls.
- L. Change and reconfiguration procedures.
 - a. The vendor will establish the process for such requests. The process must be in accordance with policy established by the State and with the State contractual arrangements.
 - i. Some types of changes (e.g. call overflow scheme) may have different change processes than other types of changes (e.g. pANI initial routing)
 - b. The vendor will determine authority of requestor to make the change.
 - c. The vendor will devise a plan for accomplishing the requested change. This plan must include but is not limited to:
 - i. Obtaining approvals from the State and other stakeholders as required

- ii. Establishing a timeline for the change that is satisfactory to the impacted parties and in accordance with policy
 - iii. Assessing the impact of the change or the reconfiguration, and assess the impact of the change process itself, on 9-1-1 operations
 - iv. Providing for the mitigation of identified impacts as required
 - v. Ensure that all stakeholders in the change process have been properly notified
 - d. The vendor will perform project management for the change or reconfiguration process.
 - i. The vendor will update all documents and records in the management system as required by the change
- M. The vendor will develop and present to the State for approval a disaster recovery plan. This plan will be invoked in the event of a catastrophic failure of all, or of a significant portion of, the 9-1-1 service, and that will require substantial time to repair or to mitigate, and that will adversely impact Public Safety.

At a minimum, this disaster recovery plan will address

- a. Persons or entities to be notified (e.g. officials, stakeholders)
 - b. Authorized messages to be conveyed in such a circumstances
 - c. Authorized actions to be or that may be undertaken by the vendor in an attempt to mitigate the catastrophic failure
 - d. Roles, responsibilities and chain of command for vendor mitigation actions
 - e. Recovery and restart procedures, involving stakeholders if needed, after the root cause of the failure has been resolved
 - f. Alternative methods of monitoring or determining the status of the 9-1-1 service should the failure limit the vendor's normal methods of IP or service monitoring
- N. The vendor will develop and publish its internal and external escalation procedures, including contact information and the chain of command.
- O. IP network change procedures:
 - a. The vendor will establish the process for requests such as for a location change, bandwidth change, facility migration, CPE replacement or other activity impacting some part of the IP network. The process must be in accordance with policy established by the State and contractual arrangements.
 - b. The vendor will devise a plan for accomplishing the requested change. This plan includes but is not limited to:
 - i. Obtaining approvals from the State and other stakeholders as required,
 - ii. Establishing a timeline for the change that is satisfactory to the impacted parties and in accordance with stated policies,
 - iii. Assessing the impact of the change and the change process on network operations, and providing for the mitigation of identified impacts as required,
 - iv. Ensuring that all stakeholders in the change process have been properly notified.
- P. pANI administration
 - a. The vendor will:
 - i. Request pANI range assignments from the service provider or make appropriate assignments itself, as requested and as required
 - ii. Maintain a database of pANI ranges and initial destination
 - iii. Manage requests for pANI ranges from service providers
 - iv. Contact service providers, as appropriate, to make changes

For future consideration, the State may choose to implement a Change Review Board to review and approve changes.

3.2.2 Network Configuration and Change Management

Vendors shall concisely describe the process and/or SOP that they use for making changes to the network and/or its configuration. Changes may include adding a connection, re-provisioning a circuit, or changing a QoS priority.

The description shall describe procedures such as how proposed changes are planned, authorized, authored, reviewed, noticed, implemented, tested, backed out, and backed up. The description shall also identify the personnel involved. The vendor's role and any State requirements in this process are especially important.

3.2.2.1 Configuration Back Up

Vendors shall describe their capability to automatically or routinely backup network configuration data, such as router and switch configurations.

3.2.2.2 Configuration Restoration

The process and conditions used to restore the configuration of network elements such as routers or switches, should the need arise, shall be described.

3.2.2.3 Root Cause Analysis

In the event of a critical or major outage the vendor shall provide State staff with a root cause analysis (RCA) within five business days. A Root Cause Analysis shall be provided upon request for minor outages.

3.2.2.4 Trouble Shooting Tools and Techniques

Vendors shall describe the tools and techniques at their disposal to perform troubleshooting and post-event analysis.

3.2.2.5 Scheduled Maintenance

The vendor shall provide a schedule of preventive maintenance activities, their frequency and strategy to continue network functionality during maintenance activities.

3.2.2.6 Maintenance Standard Operating Procedure

Any maintenance by vendors, including upgrades to the network, shall be conducted in accordance with a mutually determined SOP.

3.2.2.7 Remote Location/Back-Up

The vendor shall assure that a remote location and its designated back up are not affected at the same time.

3.2.2.8 Support Logs

The vendor shall use support logs to drive the development of solutions to recurring issues.

3.2.3 Security Monitoring and Management

Security monitoring and management shall be quoted separately from other monitoring and management services.

3.2.4 Monitoring, Alarming, and Trouble Reporting

Monitoring and reporting functions require coordination with third-party service providers, internal network requirements, connecting networks and the NG-911 routing services. Monitoring functions that overlap should be given due consideration. Monitoring should not place an onus on the ability to provide service, as some monitoring practices have the potential to utilize bandwidth to the point of potentially adversely impacting core functionality.

3.2.5 Security

Security for ESInet shall use a layered security approach with defined and protected network boundaries. The ESInet shall be partitioned into distinct IP security domains. Each IP security domain is defined as an interconnected set of IP subnets within which IP packets may be freely exchanged among the connected IP hosts and IP gateways within that domain. Internet Protocol packets which enter or leave a security domain shall traverse firewalls capable of enforcing the security requirements of that domain and which are able to detect and alarm intrusion attempts which violate the security domain's policies.

The following IP security domains are defined:

1. Core ESInet Zone – This security domain will observe the highest levels of security. Instances of the ESRP, ECRF, Policy Routing Function (PRF), and other functions critical to the overall delivery of emergency calls shall be located within this security domain. LNGs that terminate incoming 9-1-1 traffic from legacy trunks (such as SS7 ISUP or CAMA trunks) shall also be located within this zone. No direct IP access to the Core ESInet Zone from the public Internet shall be permitted. Any connection between the Core ESInet Zone and the public Internet must be indirect via application-level relay devices located in a Demilitarized Zone (DMZ) or PSAP zone, described below.
2. A DMZ is any security zone that may connect to the public Internet via an intrusion-detection capable managed firewall, and which connects to the Core ESInet Zone via a similar but physically distinct managed firewall. Any IP traffic to or from the public Internet which must access hosts or services in the Core must terminate on application gateways in this security zone which relay the traffic into the core. Servers which provide information that is to be made available via the public Internet, such as instances of the Location Verification Function (LVF) shall be located in a DMZ.
3. PSAP domains are IP-based LANs at ESInet-connected PSAP sites. PSAP domains are, from a security perspective, treated like DMZs, except they are operated by the PSAP or its suppliers, rather than the NG-911 Core network operator. In any case, the core operator shall provide and operate managed firewalls which connect PSAPs to the core ESInet.
4. Public Internet – The public Internet represents any IP domain (but not a PSAP domain) that has no security mechanisms, or over which the operator of the core ESInet has no control. The public Internet domains shall be viewed as a source of extreme security threats.

A basic policy of firewall configurations is that direct IP packet communication from public Internet domains to/from the Core ESInet domain is not permitted. Rather, all public Internet to Core ESInet communications shall be performed by application-level relay devices which operate in a DMZ or PSAP domain.

For example, a back-to-back User Agent type SIP Session Boarder Controller may be located within the DMZ, which would terminate a SIP call originating from the public Internet on one side and re-originate that SIP call on the other side toward the

core. The Internet-facing firewall will permit Internet communication with only one side of the SBC while the core-facing firewall will permit communication only between the other side of the SBC and the Core ESI-net security domain. If provisioned, such a public Internet SBC shall be a separate and physically distinct device from other SBCs used within the ESI-net.

Any interface to the public Internet, such as the Internet side of the DMZ firewall, may become the target of a Denial-of-Service (DOS) attack. Public Safety applications which depend on connections to the Public Internet must be able to tolerate intervals of limited or diminished performance without adversely affecting the ability of the public to initiate emergency calls from non-public Internet sources. For example, calls delivered via CAMA or SS7 trunks to Core LNGs shall not be impacted by a DOS attack on DMZ hosts.

The public Internet may be used to obtain non-critical status information about the ESI-net. For example, authorized personnel may remotely access, manage, and maintain certain aspects of the emergency call delivery system via application-specific relay servers located in a DMZ. Such authorized employees might be able to log into a DMZ network monitoring server from their homes via the public Internet. The DMZ network monitoring server replicates certain network status information that it obtains from status servers operating in the Core.

Finally, encrypted tunnels, VPNs, or other techniques for carrying private and secure IP traffic over the public Internet may be utilized as a communication link in the public safety solution, but only as a 2nd or 3rd level backup or fallback for required dedicated facilities. Specifically, if geographic redundancy is a requirement in some portion of the ESI-net, then such public Internet-based communications links may not be used to satisfy the redundancy requirement. However, a public Internet-based link might be utilized as a 3rd communication link to provide additional resiliency, provided all parties are satisfied with the security of such a link.

4. OHIO GEOGRAPHIC INFORMATION SYSTEM

Geographic Information Systems play a far more critical role within the NG9-1-1 environment. Today, GIS is primarily used within the dispatch mapping modules in CAD systems once the call reaches the PSAP. Within NG9-1-1, GIS data is applied at the first stage of the call and all calls will be routed based on location using GIS datasets to determine the proper routing to ESInets and PSAPs.

Geographic information system-enabled call routing requires accurate and up to date GIS data. It is imperative that local GIS data adhere to the proper data standards and then an effective plan for data maintenance is implemented. This section outlines the steps that need to be taken to meet the GIS requirements for call routing and location validation in a NG 9-1-1 environment.

4.1 Geographic Information System Standards

Standards for GIS data are essential to maintaining integrity across GIS data for 9-1-1, as well as promote data interoperability across 9-1-1 authorities. It is highly recommended that a Statewide NG 9-1-1 GIS data standard be established to provide a single database standard that follows the approved NENA standards that local 9-1-1 authorities can adopt and implement within their own local systems to assist with the preparation of GIS data for NG9-1-1. The GIS database standards need to be developed to include the foundation of the existing NENA 9-1-1 GIS standards that are currently available. The standards also need to include the scalability of database standards for future NG9-1-1 systems. NENA will be releasing a new GIS Data Model 2.0 in the future; however that document is still going through review processes prior to any final release. The current NENA Standard Data Formats for ALI Data Exchange and GIS Mapping 02-010 v9, NENA GIS Data Collection and Maintenance Standards, 02-014, as well as the NENA Detailed Functional and Interface Standards for the NENA i3 Solution (TSD), 08-003 v1 should be considered when developing the Statewide database standards. NENA document 08-003 has a GIS Layer Definitions section in Appendix B which includes fields that will need to be considered for NG 9-1-1. The statewide standards should outline fields that are required to be populated at this time for call routing and validation and what fields are currently optional but could become required as NG9-1-1 evolves.

The state of Ohio currently has a linear based referencing system also known as the Location Based Response System (LBRS) which is sponsored by the Ohio Department of Transportation and administered by the Ohio Office of Information Technology's Ohio Geographically Referenced Information Program (OGRIP). LBRS has established partnerships between State and local governments for the development of spatially accurate street centerlines with address ranges and site-specific address locations that have been field verified. Currently there are over 75 counties participating in the LBRS program. The current LBRS standards include many of the currently required fields for street naming, address ranges, addresses and political jurisdiction names that would be included as part of the statewide NG 9-1-1 GIS standards to be developed. With many counties having adopted the LBRS standards for their GIS data, the initial implementation of GIS data to a new statewide NG9-1-1 database standard will be made easier for those counties. It is recommended that the State incorporate LBRS fields into the new Statewide NG9-1-1 GIS database standard to then only have one GIS addressing model across the State. For State agencies or counties that do not need to use certain fields, those fields can be left blank or removed when utilizing in systems that do not require them. For example, when data is sent from a local 9-1-1 authorities to a database for ECRF or LVF purposes only the fields required for that NG 9-1-1 application would need to be included and not any additional LBRS field but when the data is sent to the LBRS program all of the LBRS fields are sent but not necessarily all of the NG 9-1-1 fields if they are not required by the Ohio Department of Transportation (ODOT).

Statewide standards will help to implement effective data maintenance and quality control of the dataset as data is utilized for call routing and location validation. Geographic information system data and regular data updates will need to be validated against a set of quality control services to check for potential errors such as missing field values in required fields and addressing anomalies that can be checked. It is highly recommended that quality control checks be implemented by local 9-1-1 authorities as part of their GIS data maintenance processes. The provider(s) for ECRF and LVF will also have specific quality control checks for data attributes, gaps and overlaps as part of the those implementations that will also provide discrepancy reports back to the originator of the GIS data. It is also recommended that additional data quality control checks be provided at a regional or state level if data is being provided to any Spatial Information Functions (SIF) at a regional or state level. The regional or state level quality control tools or processes could be implemented as secured web services that could be accessed by local 9-1-1 authorities. The services would provide a discrepancy report back to the local 9-1-1 authorities outlining any specific errors or warnings that the local 9-1-1 authorities will need to address. This would provide additional levels of quality control prior to the data being replicated to the ECRF and LVF. The 9-1-1 authorities will be responsible for reviewing and remediating any discrepancies that are reported through ECRF and LVF or state or regional level SIF quality control processes.

4.2 Synchronization of Geographic Information System data with Master Street Address Guide and Automatic Location Identification Databases

An important step in the preparation of GIS data for NG 9-1-1 is the synchronization of GIS data with the Master Street Address Guide (MSAG) and ALI databases. It is highly recommended that 9-1-1 authorities begin the process of comparing the addressing information between their GIS data layers and MSAG and ALI, if they have not begun that process already. The NENA technical document 71-501 for Synchronizing Geographic Information System databases with MSAG and ALI provides guidelines for the synchronization process. This process will identify any inconsistencies across the datasets such as inaccurate address ranges, improper road naming conventions, incorrect community names or ESNs. To effectively route and validate addresses in a NG 9-1-1 environment it is critical that these databases be consistent with one another. The National Emergency Number Association recommendations, outlined in Technical Standard 71-501, call for a 98 percent match rate¹ between GIS road centerline and MSAG to improve overall accuracy of the databases and in preparation for NG91-1. These steps in the preparation of GIS data will help in the transition to a spatial MSAG where the MSAG is replaced by the GIS road centerlines. Over the long-term, the transition to NG 9-1-1 will see the information in the LIS and ECRF replacing ALI and MSAG for call routing.

The ALI database is compiled with fields from the telephone company's customer record information system (CRIS). Included in the ALI database are fields with customer name information and unlisted telephone numbers which limits the dispersal of copies of the ALI database without at minimum a non-disclosure agreement in place. For effective synchronization of ALI, MSAG and GIS databases it would be beneficial to consider options to provide 9-1-1 authorities with access to specific address information within the ALI database to perform regular validation between GIS, ALI and MSAG. These options could include, but are not limited to:

¹ NENA Information Document for Synchronizing Geographic Information System databases with MSAG and ALI, NENA 71-501, Version 1.1, September 8, 2009, page 17

- The state of Ohio and the telephone companies that provide ALI database, entering into agreements for those companies to provide regular extracts of the ALI database for a Statewide database that would be managed by the State in the State of Ohio Computing Center (SOCC). This would allow the State, or a vendor hired by the State, to manage a Web service that would allow 9-1-1 authorities to query their data against the ALI database records without each 9-1-1 authority to have a copy of the ALI database. The agreement between the State and the telcos would only need to consider the addressing information in the ALI database and not require the customer name information from the ALI database in order to perform synchronization services. There are current issues with data sharing laws that need to be resolved moving forward.
- A second option would be to have the telcos required to synchronize their ALI database records against the LVF on a regular agreed upon interval where the accuracy of the ALI database could be monitored by the State 9-1-1 Administrator. This would also allow for discrepancy reports between the entire ALI database and the GIS data to be available to the telco, the 9-1-1 authority and the State to maintain datasets to the required accuracy levels.

The architecture for validation in a NG 9-1-1 environment needs to consider each potential address change and how change requests and discrepancy reports are managed. For example, changes in the GIS data such as a road name change will need to trigger changes in the ALI database to ensure that the road name change is reflected in the ALI records.

4.3 Data Provisioning and Interoperability

The 9-1-1 authorities will be responsible for providing their GIS datasets to the authoritative ECRF and LVF that covers its service area for call routing, including civic addresses. The ECRF and LVF will require the GIS datasets necessary to query civic addresses, which includes at minimum, road centerlines. It is recommended that all local 9-1-1 authorities provide site address points to provide a more granular civic address query result. It will be the responsibility of the 9-1-1 authorities to provide data that meets the statewide NG9-1-1 GIS standards and accuracy levels required for the NG 9-1-1 call routing and location validation functions through the statewide ESInet and any local ESInets for its service area. The 9-1-1 authorities can determine how they will handle GIS data updates, either through their own staff, a county or city GIS department, or a vendor.

For effective data interoperability and public safety operations it is highly recommended that data be shared between local 9-1-1 authorities and the State. Data sharing already exists through memorandum of agreements between many of the counties and OGRIP through the LBRS program. It is recommended that the State 9-1-1 administrator coordinate with the local 9-1-1 authorities to share GIS information for Public Safety services and leverage existing data sharing programs by working with OGRIP to implement a program statewide. By having a copy of the local GIS data be stored within a geodatabase within the SOCC it will provide additional data backup for call routing and location validation, as well as data interoperability in case of large emergency events. It is also recommended that users from local 9-1-1 authorities would be able to access a data export utility that would allow them to export local datasets of their surrounding area to utilize in their 9-1-1 system to increase GIS data interoperability. The stored query could be accessed through a secured Web interface available to PSAPs.

4.4 Emergency Call Routing Function and Location Validation Function

The Statewide ESInet will include ECRF and LVF services for call routings and location validation functions. The GIS data layers that will be required for the state level ECRF and LVF to direct calls to the appropriate local or regional ECRF and LVF include but are not limited to the following:

- State boundaries
- County boundaries
- PSAP boundaries

- Municipal boundaries
- Coverage area boundaries specific for the ECRF/LVF

Additional data layers such as parcels or sub-parcels, if available, could also be leveraged for call routing and validation in the future. Providing any additional location reference layers such as these would need to be coordinated between the 9-1-1 authority and the provider of the ECRF/LVF for their service area. A NENA workgroup is currently developing a technical document for the provisioning and maintenance of GIS Data to ECRF and LVF and it should be reviewed upon its release for any updated technical standards or guidelines about GIS data layers for ECRF/LVF.

For purposes of redundancy or local queries, administrators of local or regional authoritative ECRFs and LVFs may also request copies of the following GIS layers from the state level ECRF. These layers will be primarily used in the state ECRF for routing to any appropriate local or regional ECRF and LVF. However, if there is a need for these layers in a local or regional ECRF or LVF, this should be coordinated through the state 9-1-1 administrator as these boundaries will be maintained through state agencies as described in section 4.6:

- PSAP boundaries
- County boundaries
- Municipal boundaries
- Coverage area boundaries for authoritative ECRFs within the state

As described in section 4.3, the local 9-1-1 authorities would provide road centerlines, site-structure points, and emergency service boundaries to the State through agreements between the local 9-1-1 authority and the State. This data sharing will provide the data interoperability required for coordination of GIS data during large emergency events and also provide data redundancy for the call routing and validation functions.

As an option for leveraging existing infrastructure and reducing costs of servers and other equipment or software costs, there may be opportunities for local 9-1-1 authorities and the State to partner to host local ECRF and LVF functions within the SOCC. Local 9-1-1 authorities would then have the option to implement their own local or regional ECRF and LVF solutions or may have the option to partner with the State to have their ECRF and LVF hosted by the State or possibly implemented within the State ECRF and LVF solutions.

4.5 Geographic Information System Data Readiness Checklist

As part of the preparation for NG 9-1-1, it is recommended that the State of Ohio provide a GIS data readiness checklist to the local 9-1-1 authorities who will outline any necessary next steps that a PSAP might need to plan during the transition to NG9-1-1. The readiness checklist may include but is not limited to

- Database standards for GIS data layers including required fields
- Best practices for data accuracy and standardized database field values
- Coordination with neighboring 9-1-1 authorities for edgematching
- Synchronization of GIS data with MSAG and ALI
- GIS maintenance planning

4.6 Geographic Information System Data Layers

Local 9-1-1 authorities will continue to maintain the primary GIS addressing datasets as those 9-1-1 authorities have the local knowledge and source information for addressing updates. For political boundary datasets, it is recommended that statewide layers continue to be maintained by appropriate state agencies. These activities can be coordinated by OGRIP. By

maintaining current statewide layers at the state level, topology and data integrity can be maintained more efficiently and updates provided to any GIS databases that are being referenced by ECRF/LVF services. These political boundaries will include, but is not limited to:

- Statewide boundary
- County boundaries
- Municipal civil division boundaries
- PSAP boundaries
- Coverage area boundaries for authoritative ECRFs within the state

For the initial development of PSAP boundaries, the State 9-1-1 administrator should work with OGRIP to coordinate a program to have those boundaries delineated and approved by the local 9-1-1 authorities. Once a seamless Statewide PSAP boundary layer has been established, the State 9-1-1 administrator should implement a maintenance process whereby the 9-1-1 authorities can notify the State of any boundary changes and once the State makes those changes, the 9-1-1 authorities affected by those changes can approve the new boundaries. As one potential option, this data maintenance workflow for PSAP boundaries could be developed an interactive map Web service that allows proposed boundary changes to be red-lined through Web mapping tools.

The local 9-1-1 authorities would be responsible for the maintenance of the emergency services boundaries representing, at minimum, fire, police and EMS. The 9-1-1 authority would need to include the maintenance of these layers within their GIS data maintenance plan and coordinate with fire, police and EMS to communicate the necessary information regarding boundary changes. The 9-1-1 authorities will also need to coordinate with their neighboring jurisdictions to resolve gaps and overlaps along each other borders. Discrepancy reports from ECRFs and LVFs will also flag any overlaps and gaps that will need to be resolved by the local 9-1-1 authority through its GIS data maintenance processes.

The balance of this page is intentionally left blank.

5. RECOMMENDATIONS

L.R. Kimball recommends the State of Ohio move forward with setting up agreements for an ESInet backbone for Statewide connectivity, as well as procuring NG9-1-1 core functionality to promote the migration to NG9-1-1 Statewide. As it stands, the Public Safety system in Ohio relies upon aging technology that is becoming antiquated. Across the country, Public Safety systems are being converted to digital technology that can provide a high level of service to the citizens and visitors to the state of Ohio. 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.

Ohio needs to keep up with ever growing citizen expectations of the 9-1-1 network. The 9-1-1 caller expects the telecommunicator on the other end of the line to know where they are and dispatch help quickly and correctly. An NG9-1-1 network will improve the Public Safety system for the citizens who call 9-1-1 and will eventually allow people in danger to reach help by other means such as text, video, social media, telematics, and more as new life saving technology is introduced. Updating technologies and implementing this new network will also assure that Ohio is prepared to support and participate in national initiatives to share critical data in the future.

This Technical and Operational Requirements document lays out specifications for an ESInet and what needs to be considered when procuring an ESInet provider, as well as describing what is needed from NG9-1-1 core functions. L.R. Kimball recommends that Ohio utilize this document to create a procurement document to obtain services to manage an ESInet.

The ESInet Steering Committee should lead the charge in creating a NG9-1-1 transition plan and cost analysis. This transition plan can be based upon the steps outlined in the State of Ohio NG9-1-1 Evaluation and Recommendations Report (May, 2013). Certain steps in this report have already been initiated. The State will need to take a look of the progress it has made since that document has been delivered and reevaluate their goals and direction.

In order to finalize an in-depth NG9-1-1 transition plan, the State will need to decide what core functionality it will be providing out to the PSAPs via the network backbone. This is a decision that will be based heavily on cost. A NG9-1-1 in-depth costing study should be conducted to determine an estimated cost of the State-provided ESInet and core functions.

L.R. Kimball also completed the Ohio Fund Analysis Report which details the current funding structure, an estimate of how much 9-1-1 costs Ohio today, and provides funding models from other states across the country, as well as recommendations for Ohio. This report is the first step in a complete NG9-1-1 costing study.

If the State can afford to provide all NG9-1-1 core functions as outlined in the technical requirements, it will then become a question of what should to State provide and what should be left to the locals. Some functions that have been discussed in several forums across the State are the State providing a CPE system and other traditionally locally based components. There are several operational impacts that would result from the state offering these functions. This decision should be made from the Technical and Operations Subcommittees, with feedback from stakeholders throughout Ohio.

Upon the completion of a NG9-1-1 transition plan and cost analysis, the State will have a strong understanding of the direction it is heading and will have a better idea of what the cost of the network and core functions will be and should then decide what they can provide in terms of functionality and connections and what will be the responsibility of the PSAPs to fund.

The figure on the following page was created for the Evaluation and Recommendations report dated May, 2013. It represents the framework of transitioning to an NG9-1-1 system and should be utilized to develop the comprehensive transition plan

along with a NG9-1-1 cost analysis. Red text within each box of the chart below represents items that the State is in the process of completing or has completed since that report was submitted.

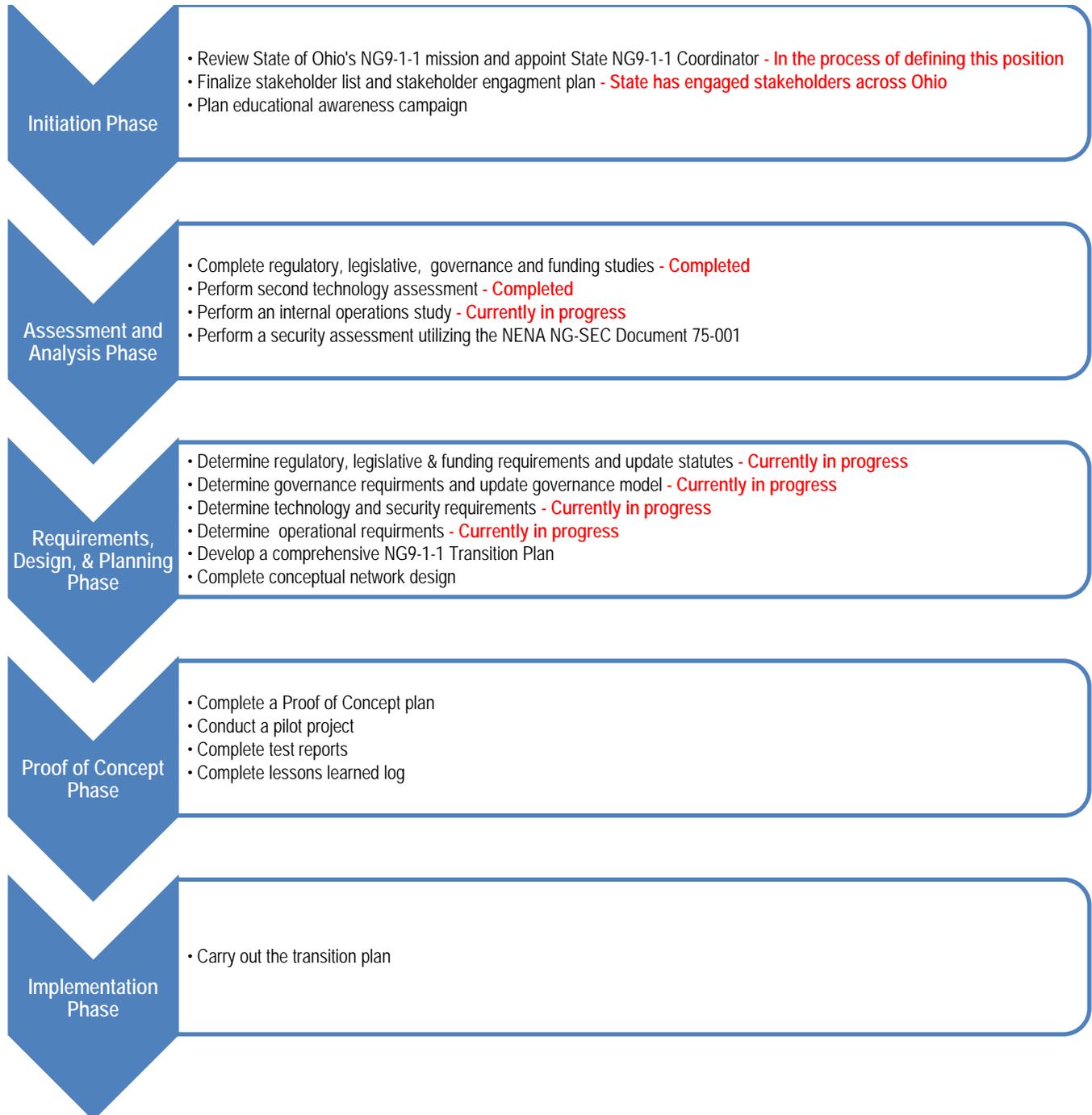


Figure 3—Transition to NG9-1-1 Framework

The figure above demonstrates the large amount of work that the State has engaged in since the Evaluation and Recommendations report was complete in May of this year. This requirements document is another step towards their goals.

The State understands that is imperative that Ohio keep its 9-1-1 system up-to-date with technology and move toward the Next Generation of 9-1-1 and has been swiftly taking steps to reach this goal.