North Carolina ESInet
Conceptual Design document

March 2016

Proprietary Notice

The remainder of this page
intentionally left blank.

Table of Contents

1. North Carolina NG9-1-1 ESInet Conceptual Design Requirements

The following subsections describe system requirements, regulations and industry standards with which the Emergency Services IP Network (ESInet) must comply as well as tasks that will be the responsibility of the Vendor. References to a vendor, vendors or selected vendor(s) in this document assumes the responsibility of monitoring and managing the quality of the products and actions to implement the ESInet.

1.1 System Service Provider Coordination Requirements

The state of North Carolina 9-1-1 Board or the Board designee must coordinate the delivery of all of the requirements for the successful deployment of NG9-1-1. In addition, the Prime Contractor must coordinate with other service providers throughout the state of North Carolina as necessary to implement and operate a seamless statewide NG9-1-1 solution.

The vendor(s) of the ESInet capabilities must in some cases acquire the services of other providers and manage and coordinate with other providers to meet the goal of NG9-1-1 throughout the State. This includes collaboration and interconnection with providers who may be delivering service to individual PSAPs connecting to the ESInet. This may also include the possibility of integrating wireline and wireless services to complete a service that offers the desired backup and redundancy necessary for NG9-1-1 communications

1.2 Interstate Interconnection Requirements

It will be responsibility of the selected vendor to ensure integrated interconnection capabilities with other System Service Providers (SSPs) in adjacent states and regional networks implemented outside of the North Carolina.

States that may require interconnection:

- Georgia
- South Carolina
- Tennessee
- Virginia

Other areas that may also require interconnection and interoperability assurances over time include:

- Military installations located within the State that have a 9-1-1 center

- Coast Guard installations

1.3 Emergency Services IP Network (ESInet) Functional Requirements

The ESInet service, solution or system design will meet the current Emergency Services IP Network Design capabilities outlined in the NENA 08-506 ESIND informational document. This information is crucial to ensure that the ESInet meets the minimum criteria for NENA i3 08-003 functionality. This document refers to NENA ESIND and i3 standards throughout to ensure compatibility.

1.4 NENA 08-506 ESIND

ESInets are like other IP networks in that they are a collection of routers and links between routers in which there are multiple paths such that failures leave at least one path that the network can use. ESInets designs, however, must meet more stringent requirements for security and reliability service levels than most other IP networks.

Per NENA i3 08-003 and for the purposes of this document we provide the following definition for ESInet:

> *"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)."***

The following list summarizes the core requirements for an ESInet, as summarized in the NENA i3 08-003:

- The network between the PSAP and an ESInet will be a private or virtual private network based upon TCP/IP

- It will have scalable bandwidth to support new enhanced services

- The Emergency Services IP Network shall be a conventional routed IP network

- MPLS (Multi-Protocol Label Switching) or other sub-IP mechanisms are permitted as appropriate

- The PSAP should use redundant local area networks for reliability

- PSAP LAN to an ESInet must be resilient, secure, physically diverse, and logically separate

- ESInets shall be engineered to sustain real time traffic, including data, audio, and video

- Connections between the PSAP and an ESInet WAN shall be secure TCP/IP connections

- ESInets should be capable of operating on IPv4 and IPv6 network infrastructures

- ESInets should consider how the Domain Name System (DNS) is designed and managed

- ESInet implementations should consider coordination efforts to understand Autonomous System (AS) number implications for statewide deployments

- ESInet configurations may impact Voice Quality

To ensure compliance with the requirements listed above, vendors should provide detailed explanations of the following technical aspects (at a minimum) of their network:

- Core routing
- Interface to Hosted solutions
- Wireless call distribution
- Text to 9-1-1 delivery
- Legacy interconnection
- ALI integration

The state of North Carolina 9-1-1 Board will deploy an ESInet configuration that aligns with the NENA i3 08-003 functional standard and includes many of the necessary components to enable NG9-1-1 and i3 functional elements to be operational.

1.5 Open Standards Based

The ESInet configuration must support multiple locations throughout the state of North Carolina. Standards for operation of the network will comprise standards that align with the Department of Information Technology and NENA. Potential vendors must ensure that their operational policies can be utilized within the framework of Department of Information Technology and NENA policies.

The State discourages the use of proprietary software, equipment and NG9-1-1 functional elements. The intent is for all applications, equipment, services and systems performing NG9-1-1 related functions to be open standards based.

Any portion of the solution that is not compliant with the policies shall be documented and identified. Any proprietary components must be clearly communicated, identified and justified with a detailed description.

1.6 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).

1.7 Industry Standards

Where applicable, all equipment and network components must comply with applicable national industry standards that allow for the implementation of technology components. This includes the appropriate cabling, electrical and wiring standards. Furthermore, the governing standard for the operation of the ESInet and NG9-1-1 is the NENA i3 08-003 standard. Appendix A lists industry standards documents to be used for reference.

1.8 Facilitating Carrier Transition

The Selected Vendor of the ESInet will be responsible for negotiating the migration of existing legacy 9-1-1 services already in service at the PSAP(s) and the migration / transition of those services onto the ESInet. The Selected Vendor will also be responsible for the creation of the necessary NG9-1-1 services at all interfaces between the 9-1-1 call originating network operators in order to accomplish a 9-1-1 call delivery which meets the quality and reliability requirements of NG9-1-1.

This may encompass agreeing to the terms, conditions, procedures, or processes for interconnection and exchange of information between other carriers' networks and systems and the ESInet.

All terms, conditions, procedures or processes will follow applicable state of North Carolina guidelines and rules as well as applicable telephone industry practices, NENA standards and recommended practices, and all applicable U.S. telecommunication law.

The State expects the Selected Vendor 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.

1.9 Entity Cooperation

The Selected Vendor must fully cooperate with additional outside entities that provide a portion of 9-1-1 service or are providing 9-1-1 service. In order to facilitate a seamless NG9-1-1 solution the Selected Vendor must anticipate sharing information, performing mutual activities and collaborating fully with other entities.

Successful respondents will provide all services necessary for the development, implementation operation, monitoring and maintenance of their proposed ESInet including:

- Design, installation, testing, interconnection and operation of ESInet components required to operate or support the operation

- Maintenance and repair of those elements of the ESInet and interconnections owned, operated, installed or controlled as part of their solution

- Completion of as built drawings, sketches and/or schematic materials related to the ESInet

- A data collection and reporting system for all ESInet elements to facilitate the monitoring, reporting and analysis of operational metrics of the ESInet

- Removal and disposal of any equipment replaced or decommissioned through the installation of the ESInet

2. ESInet Architecture Overview

Vendors must document the specifications of the ESInet in standard terminology defined by NENA. The ESInet will require a vendor to identify and document exactly how ESInet is implemented and provide assurances that the configuration meets the specification guidelines in a standardized approach. Figure 1 shows the expected ESInet configuration.

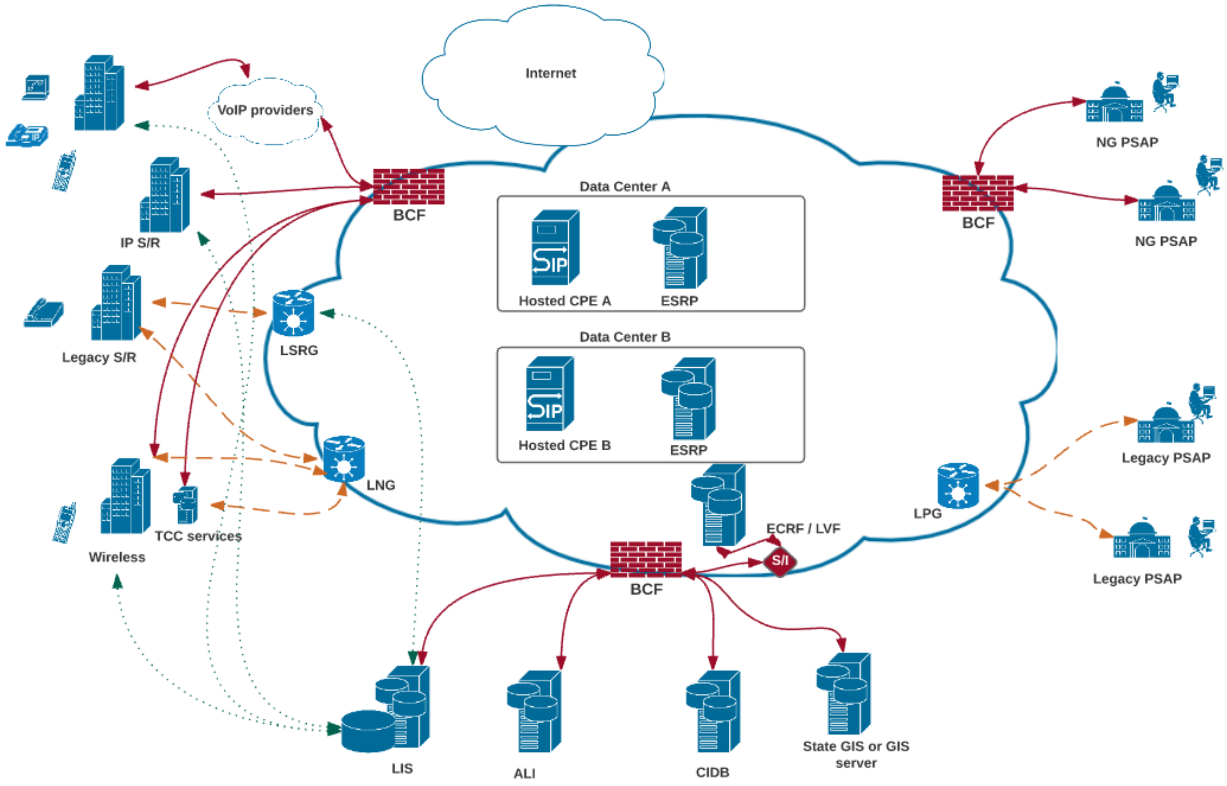

Figure 1 – Expected North Carolina ESInet configuration

The ESInet configuration must:

- Ensure that the ESInet conforms to OSI (Open Systems Interconnection Model) Layer 1 physical, Layer 2 switching and Layer 3 transport architecture.
- Enable the delivery of IP packets between nodes on the network.
- Provide a long term scalable infrastructure to support NG9-1-1

The ESInet will be configured to support delivery IP packets from any IP address to any other IP address among any and all connected sites reachable from the ESInet. This includes the possibility of having an external connection via the Internet.

Any combination of physical network communication facilities may be used within the context of providing secure, redundant, reliable and available IP communications that meets or exceeds the industry standards and the specifications.

- The ESInet design shall require a minimum level of bandwidth to support delivery of calls and associated data from originating service providers or other integrated ESInets to the PSAPs.
- The ESInet design and deployment shall use a highly reliable and redundant architecture.
- Availability, diversity, redundancy and resiliency shall be the guiding ESInet design principals
- The ESInet design shall support the ability to automatically reroute traffic to alternate routes or systems in order to bypass network outages and system failures.
- The ESInet design shall offer the ability to prioritize critical traffic at multiple levels by importance of applications or users
- The ESInet design shall be scalable and have the ability to scale without adverse effects on performance or costs
- The ESInet design shall support a guaranteed Quality of Service (QoS) level
- The ESInet design shall support the automatic adjustment of traffic priorities in order to meet established QoS levels as defined in NENA 08-003
- The ESInet design shall support the ability to ensure performance through the use of traffic shaping and traffic policing.
- The ESInet design shall support operation on a 24x7x365 basis.
- An ESInet design that utilizes the most cost effective and feasible combination of transport technologies available to deliver the bandwidth required
- The ESInet design shall support the ability to handle legacy 9-1-1 calls and ensure the capability of handling future call types

2.1 Infrastructure

The ESInet infrastructure design utilizes a combination of layers within the OSI framework. The OSI model is useful in identifying an open standard for interconnection devices and establishing a method for communication among disparate networks and systems. Figure 2 provides a diagram of the ESInet interconnections.

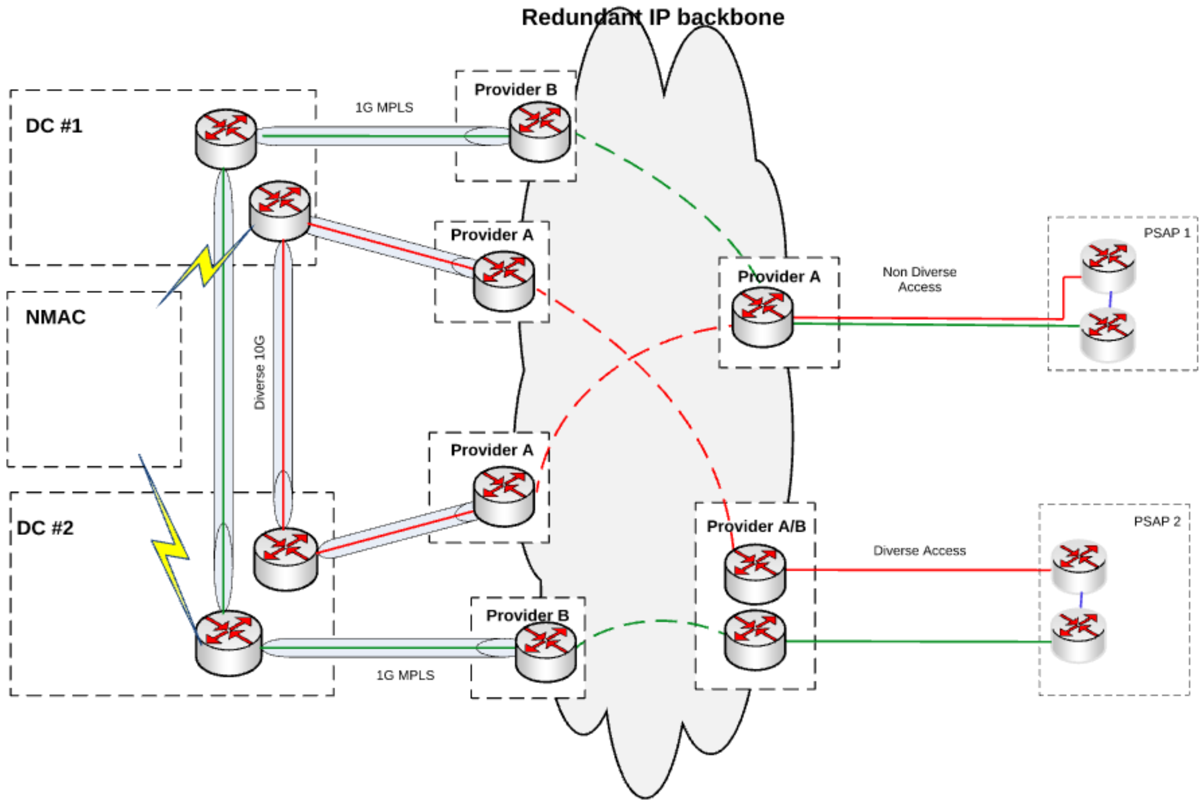

Figure 2 – ESInet interconnections

The infrastructure is also a combination of physical and logical components configured to create the NG9-1-1 services. It is important to recognize that an NG9-1-1 design utilizes several component parts connected by the common ESInet. The result is a seamless ecosystem that operates for the specific purpose of delivering 9-1-1 calls through the network to the PSAP. Therefore the NG9-1-1 ecosystem contains several disparate connections, devices and services that when combined provide NG9-1-1. They are:

- Physical network
    - Transport connectivity
        - Entrances

            - Diverse
            - Single entry

        - Cabling and Wiring
        - Local Area Network interface (demarcation point at PSAP)

- Logical network
    - Routing and switching
        - Routing protocol support
            - OSPF
            - BGP
            - RIP
            - EIGRP
        - Routed protocol support
            - TCP/IP
            - UDP
            - SIP
        - Switching
            - Ethernet
- ESInet network
    - Wide Area Network (WAN) network support
        - Across demarcation points
        - Across multiple providers
        - Legacy network interconnections
    - Local Area Network (LAN) interface
    - Core functional networks and access
        - ECRF
        - ESRP
        - PRF
        - Legacy Gateways
        - Legacy call delivery systems
        - NG9-1-1 call systems
- NG9-1-1 service

  - Comprised of all components
    - Physical
    - Logical
    - ESInet
    - Data Center monitoring and operation
    - Service management
  - Call delivery system
    - CPE
    - PSAP communications system
    - Vendor interface
- Service Management architecture and infrastructure management
  - Availability management
  - Reliability management
  - Capacity management
  - Service continuity management
  - Security management
  - Supplier management
  - Service configuration database and library management
  - Risk management
  - Compliance management
- Service Management administration and operations management
  - Configuration and knowledge management
  - Project management
  - Change management
  - Release and deployment management
- Service Management operation and improvement management
  - Help Desk
    - Event management
    - Incident management
    - Problem management
  - Access management
    - Identity, Access, Rights management
  - Operations control
  - Information assurance support
  - Service review

- Service Level Agreement (SLA) adherence

In particular the ESInet design must adhere to the OSI model. Therefore, the ESInet will require the functionality provided specifically by the OSI Layer 1, Layer 2 and Layer 3 for the foundational connectivity.

The Selected Vendor must be prepared to include OSI Layer 1, Layer 2 and Layer 3 facilities that may be required to interconnect to the End Sites.

The Selected Vendor must clearly identify the OSI Layer 1, Layer 2 and Layer 3 facilities in a network diagram and explain the connections, interfaces and configuration to document how the ESInet utilizes them.

Design of OSI Layer 3 services must meet the service level agreement (SLA) metric defined in the SLA which must in turn be designed to meet the NG9-1-1 standards and protect the entire ecosystem.

2.2 Routing Protocols

The ESInet will be configured as an OSI Layer 3 IP network. The IP network uses routing protocols defined in this section to control traffic and assist in the delivery of data. The ESInet vendor must also implement a dynamic interior gateway IP routing protocol for routing inside the IP network. The best solution for this is Open Shortest Path First (OSPF). The network also requires an exterior gateway protocol for routing to outside agencies, partners, and providers. The preferred standard is Border Gateway Protocol (BGP).

All standard protocols that use IP for transmission must be transported over the network. No specific protocol or use of the IP network may be blocked or inhibited by the ESInet provider, except to comply with specified security policies. Vendors must ensure that their network design supports this capability. Figure 3 is a visualization of protocol interaction.

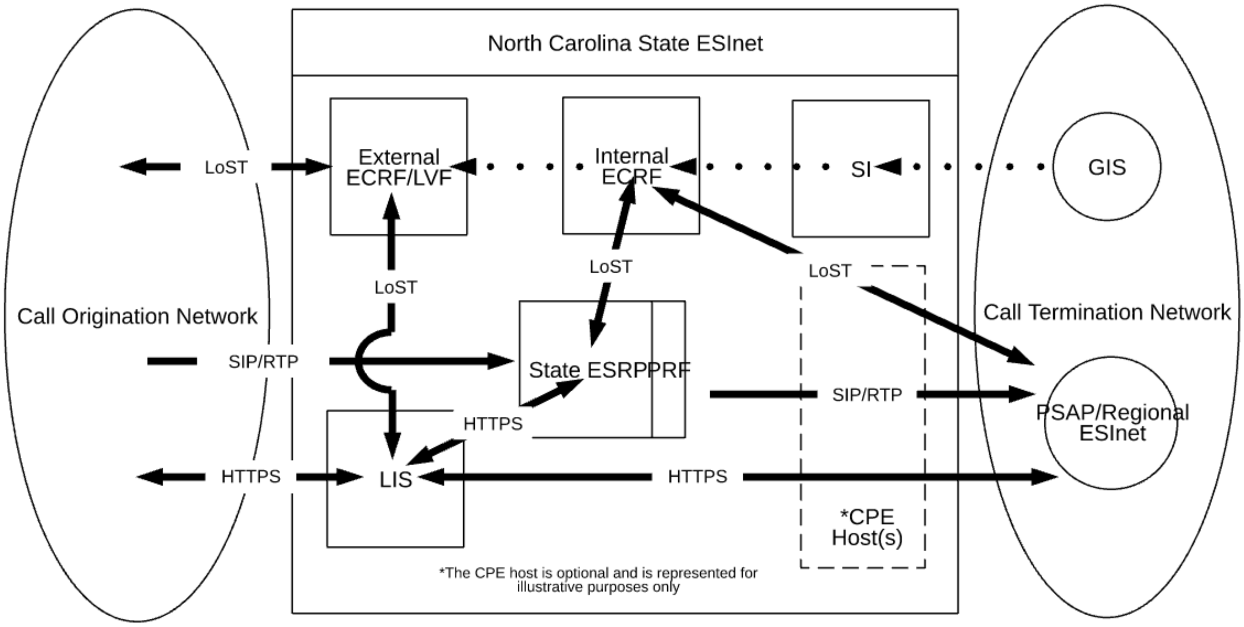

Figure 3 – Protocol Interaction

The ESInet will utilize the following Routing Protocols:

- The most common method for deploying the ESInet is to utilize Open Shortest Path Forward (OSPF) internal to the ESInet. OSPF allows for rapid selection and transmission to a preferred route inside the ESInet. The NENA i3 standard recommends that OSPF be utilized where possible to allow for interconnection among many ESInet installments.

- External networks in the ESInet will utilize the Borger Gateway Protocol (BGP). BGP is a standardized protocol that allows disparate networks the ability to interconnect and transfer IP packets.

- Other methods such as the Routing Information Protocol (RIP) and the Enhanced Interior Gateway Protocol (EIGRP) should be avoided. If these protocols are used, the vendor will be required to explain their use and all protection from network issues due to their usage.

2.3 Routed Protocols

Routed protocols may be necessary to establish the environment required to deliver voice calls via IP across the ESInet.

2.3.1 Transmission Control Protocol/Internet Protocol (TCP/IP)

The ESInet will use TCP/IP as the primary transport protocol within and between all functional elements within the ESInet. TCP takes care of reliability issues for IP networks by ensuring that the flow of packets is consistent. If TCP identifies an error, it will either slow or stop the flow of packets automatically until the error is corrected. For this reason, TCP can introduce delays due to retransmitting packets into an unacceptable level of jitter for the end user.

2.3.2 User Datagram Protocol (UDP)

The UDP will be the method of choice for all voice traffic within the network. UDP is a connectionless protocol which transmits data packets without any negotiation, setup or warning through the network to the termination device. UDP requires no handshake or setup; it just packets of data. UDP also does not perform error control on the data that it transmits. It may deliver packets in an incorrect order or it may even leave them out entirely. While this seems like a potential problem, UDP is better for applications that require a constant, steady stream of information rather than ensuring that every single packet is received. For this reason, and the factors surrounding the potential delays due to error correction and reliability with TCP/IP; UDP is ideal for real-time communications.

2.3.3 Session Initiation Protocol (SIP)

NG9-1-1 call delivery has been standardized on the SIP. The call processing equipment uses SIP as the primary method of delivering the call and data required for 9-1-1 from end to end in an NG9-1-1 system. SIP was initially designed to expedite the call set up for real time multimedia sessions between many users or end sites. This means that SIP is appropriate for potentially all forms of communication (voice, text, video, other multimedia).

SIP is also a general purpose type routed protocol that assists:

- User location and registration
- User availability
- User capabilities
- Session setup
- Session management

2.4 Architectural Survivability

The ESInet core network and the interconnection to any NG9-1-1 core functional element will be redundant with high survivability. This requirement specifies that the implementation of nodes must also be a survivable node on the network. The architecture must be able to survive the total destruction, such as by fire or flood, of any one Core Network site, a switching center, data center or interconnection site.

This includes the event of a "sunny day" situation. A "sunny day" is a day in which no significant events occur in the state of North Carolina; however, an event may occur somewhere else in the United States that could impact the system in operation in North Carolina. Vendors must ensure that events that never directly occur within North Carolina will not affect their architecture.

2.5 Network Diversity

Diversity will be implemented as much as possible and where it is reasonable to do so. In most cases this will require a new connection or diverse entry into an end site. If the cost of providing a physical connection is excessive, or problematic the vendor may provide an alternative method such as a wireless option.

Where complete diversity is not available, the vendor must document the location and provide details surrounding the network connection and risk associated with the particular location.

The network core solution and redundantly connected sites shall include physically diverse routes and physically diverse building entrances. Where diversity is not feasible, the vendor must provide an alternative.

Vendors proposing elements not provisioned with physical diversity shall document these elements and discuss them with the state of North Carolina NG911 Board and present and explain alternatives.

2.6 Network Availability and Reliability

The ESInet design must provide 99.999 percent (five-9's) availability of access to the NG9-1-1 functional elements. For the purposes of providing this level of availability, the definition of the ESInet is that part of the demarcation point at the PSAP to the ESInet and the transport network through the ESInet core. The Selected Vendor will report on their adherence to the SLA metric on a monthly basis.

Calculation of this metric must include scheduled and routine maintenance activities. During maintenance activities that may impact any functionality on the network the Selected Vendor must implement a solution to avoid any potential downtime prior to conducting the maintenance task.

The 99.999 percent metric assumes full redundancy and diversity is achieved and maintained. Therefore, vendors must plan to deploy all functional elements in a diverse and redundant manner. Alternatives may be necessary in some areas to ensure that the availability meets the five 9's (99.999) metric.

Network availability will be implemented to meet the 99.999 percent goals of reliability and availability as defined:

> *Reliability is the ability of a system or component to perform its required functions under stated conditions for a specified period of time.*
>
> *Availability is the degree to which a system or component is operational and accessible when required for use.*

Any predictable maintenance or upgrade process affecting hardware, firmware or software that would require the proposed solution be removed from service for any length of time must be identified and communicated to the state of North Carolina.

Availability will be measured according to the following calculation:

$$A = \frac{UpTime}{(UpTime + DownTime)}$$

Reliability will be measured according to the following calculation:

$$R_a = \frac{Successes}{Attempts}$$

The ESInet must maintain a reliable and available platform for all PSAPs to utilize and to interoperate with the NG9-1-1 functional elements at the core of the ESInet.

2.7 No Single Point of Failure

The design and implementation of the ESInet must have no single point of failure and any selected vendor(s) must document measures used by the vendor to achieve this threshold. The selected vendor(s) must ensure that their ESInet meets the service resiliency and redundancy appropriate for 9-1-1 call delivery per NENA standards.

2.8 Service Level Agreements (SLA)

The ESInet vendor will be required to develop and support a service level agreement (SLA) that specifies the performance requirements for the ESInet and all components as deployed at any time. It will be the vendors' responsibility to disclose risks to achieving the SLA (99.999 percent) throughout the lifecycle of the system.

The vendor will provide visibility to the vendor Network Operations Center (NOC) to the Network Monitoring and Assistance Center (NMAC) for the purpose of having a collaborative, coordinated approach for managing the service.

If there is an exception within the SLA report, the NMAC will escalate to the NG911 Board or the Department of Information Technology for support and resolution.

Vendors must provide a description that includes details such as (but not limited to):

- Schedule of SLA reporting
    - The ESInet vendor will supply monthly statistical reports documenting their adherence to the SLA to the NMAC. The reports may include the following:
        - Service Level Achievement and Monitoring (SLAM) charting
        - Review of issues and incidents
        - Service improvements
        - Potential IT changes to existing service
- Problems will be discussed with the NMAC. Problem areas may arise from many sources. This is a partial list of potential problem areas to be regularly discussed:
    - Hardware issues
        - Servers
        - Switches
        - Routers
        - Other defined hardware components utilized within the service
    - Software issues
        - Operating system software issues
        - Security system software issues
        - Other software defined within the solution that may be impacted

- Connectivity issues
- Coordination with other carriers networks, services and systems that may impact the system
- Continuity issues

The ESInet SLA may include the common Information Technology Infrastructure Library (ITIL) framework for tracking, responding to, and reporting on network and system outages or failures:

- Severity Level 1 Incidents resolved within 4 hours
- Severity Level 2 Incidents resolved within 8 hours
- Severity Level 1 and 2 Incidents responded to within 30 minutes
- Severity Level 3 Incidents resolved within 48 hours
- Severity Level 4 Incidents resolved within 96 hours
- Problems resolved within applicable time frame

Severity 1 Incident

- An incident shall be categorized as a "Severity 1 Incident" if the incident is characterized by the following attributes:
  - Renders a business critical system, service, software, equipment or network component unavailable or substantially unavailable, or seriously impacts normal business operations, in each case prohibiting the execution of productive work,
  - Affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

Severity 2 Incident

- An incident shall be categorized as a "Severity 2 Incident" if the incident is characterized by the following attributes; an incident that:
  - Does not render a business critical system, service, software, equipment or network component unavailable or substantially unavailable, but a function or functions are not available, substantially available, or functioning as they should, in each case prohibiting the execution of productive work

  - Affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

Severity 3 Incident

- An incident shall be categorized as a "Severity 3 Incident" if the incident is characterized by the following attributes:
  - An incident causes a group or individual to experience an incident with accessing or using a system, service, software, equipment or network component or a key feature thereof and a reasonable workaround is not available, but does not prohibit the execution of productive work.

Severity 4 Incident

- An incident shall be categorized as a "Severity 4 Incident" if the incident is characterized by the following attributes:
  - An incident may require an extended resolution time, but does not prohibit the execution of productive work and a reasonable workaround is available.

The 9-1-1 Board expects all of the ESInet network components and functional elements and any associated service will perform at the level of 99.999 percent uptime. NG9-1-1 administration will measure failures to meet SLAs per service affecting outage and will assess penalties for failure to meet SLAs.

For Severity Level 1 and 2 incidents, the assessment shall be 10 percent of the monthly recurring charge (MRC) as a penalty whenever the outage exceeds the initial period of resolution.

If the resolution period length of time doubles, then the penalty shall increase to 20 percent. Resolution period length of time in excess of four times the initial period will result in 50 percent of the MRC being waived.

- SLA Violations
  - An SLA violation shall have occurred whenever:
    - The ESInet reliability and/or availability and/or performance fails to meet any single performance metric, or
    - The average of any single performance metric over the preceding 2 month period fails to meet the service level. This is an "early warning" of an unacceptable trend.

- SLA Violation Damages
  - Damages shall apply whenever:
    - Any single performance item SLA violation occurs for two consecutive months.
    - Any single performance item SLA violation occurs the month following an occurrence of an SLA violation.

2.9 Network Configuration

Documentation delivered to the NMAC will accurately portray the ESInet network and complete configuration of the core components. This includes a network diagram showing the components, interconnections and methods of connection at all end sites.

The NMAC will be the primary point of contact for the vendor for any network configuration or support for the ESInet.

Vendors will be required to populate a Configuration Management Database (CMDB) that the NMAC will consolidate to operate as a complete library of all components of the network. The NMAC must keep this database current with information provided by the vendor(s). This system may include but not be limited to diagrams, routing addresses, software version information and current model / revision numbers of all components.

The network diagram and any accompanying clarification must include enough detailed information regarding the configuration to allow for the NMAC and potentially the Department of Information Technology to verify and validate that the ESInet meets the specification. In addition, the NMAC will treat the network diagrams presented as "As-Built" information and will require maintenance by the vendor as the vendor completes changes to the network.

- Network diagram(s) must be clear and easy to understand.
- All diagrams should; at a minimum, clearly show the core network and the site connection(s) so that the topology and design and the selection of the Layer 1, 2, and 3 technologies are clear.

2.10 Quality of Service Features

The ESInet design must meet the quality of service (QoS) features suitable for the real-time transport of Session Initiation Protocol (SIP) traffic. This includes the ability for a calling party to request emergency services over multiple devices and technologies.

NENA i3 standards provide the framework for SIP-based call transport and must be followed. Any deviation or discrepancy between NENA i3 and the vendors' service must be documented and reviewed by the state of North Carolina 9-1-1 Board and the Department of Information Technology prior to implementation of such a service.

The following network performance requirements are taken directly from NENA 08-506, Version 1, December 14, 2011, and are highlighted to provide a basis for establishing a performance based network:

Packet Loss

It is a best practice to engineer ESInets to keep the packet loss budget under 2.5 percent. ESInets designs should have no oversubscription. Packet loss of less than 1 percent should be achievable on such ESInets.

Jitter

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

Latency

The maximum acceptable delay for packets traversing the ESInet should be less than or equal to 35 mS. It is a best practice to design ESInets to operate with less than 15 to 20 mS of latency. This allows the original encode and decode and a conference bridge in the middle of the path and still achieves the maximum 35 mS or less packet delay.

2.11 Traffic Prioritization

Traffic within the ESInet may be prioritized to ensure a minimal delay, especially for voice communication. The ESInet vendor must provide a description of their methodology for traffic prioritization and document how the prioritization interacts with QoS and the IP routing protocols.

- Real time traffic includes the 9-1-1 call and associated data.
- Non real time traffic may require dynamic prioritization.
- The QoS methodology and configuration should allow for the ability to alter the priority within the system, such as Session Initiation Protocol (SIP), if needed.

2.12 Real-time Transport Protocol Streams

The delivery of IP-based voice calls via SIP rely on the Real-time Transport Protocol (RTP). RTP streams must be configured within the ESInet to minimize excessive latency and jitter throughout the network. The vendor must provide assurance that their usage of RTP enhances the QoS structure and reliability of SIP delivery throughout the ESInet.

The vendor must include a QoS structure or IP routing scheme that reduces the sharing of bandwidth of RTP sessions on the redundant links.

This ensures that RTP packets in user datagram protocol (UDP) streams arrive at the destination in sequence in the event that the redundant links have latency issues.

2.13 Network Facilities

The ESInet network and communication facilities implementation must allow seamless connection between the end sites and the network to interface with the NG9-1-1 functional elements. Vendors must describe any potential facilities necessary to create the interface to the functional elements for NG9-1-1. The vendor must provide the NMAC with both a narrative and diagram documenting all network facilities to ensure that all component facilities and demarcations are known.

2.14 ESInet Interconnections

The ESInet will interconnect to a minimum of two data centers and allow communication between the end sites and the NG9-1-1 functional elements. The ESInet may also contain connections to devices and functional elements that reside outside the ESInet. All interconnections, whether to the core or to outside resources, must be redundant and diverse and provide survivable features that can meet the 99.999 service level as identified in Section 2.6.

- The Core Network design must sustain IP traffic without limitations assuming all potential PSAP and end site interconnections such as a Legacy Network Gateway or Legacy PSAP Gateway.

- At each redundant PSAP or end site, the demarcation interface to the site's local area networks (LANs) shall be two redundant 100-Megabit or faster Ethernet ports.

Legacy Network Gateway

The ESInet will employ a Legacy Network Gateway (LNG) at the interconnection point between the ESInet and a legacy network provider. The LNG interconnect will do the following:

- Will provide a bridge between existing origination network and ESInet.
- The LNG will provide a legacy selective router type interface towards the origination network (such as ISUP or CAMA), and provide a SIP interface towards ESInet.
- The LNG will be located outside of the ESInet and route according to the Emergency Call Routing Function (ECRF). The LNG will also utilize the Emergency Services Routing Proxy (ESRP) for routing instructions. The LNG routing must come through the Border Control Function (BCF) before it delivers payload to the ESInet.
- The LNG implementation must allow location Interwork.
- The LNG uses the SIP/HELD interface for Location by Reference towards the ESInet.
- The LNG will be a permanent part of NG9-1-1, as long as legacy origination networks are deployed

Legacy PSAP Gateway

The ESInet will employ a Legacy PSAP Gateway (LPG) at the interconnection point between the ESInet and a PSAP that is not yet capable of NG9-1-1 call handling.

- The LPG configuration will allow existing, un-upgraded PSAPs that are operating with legacy 9-1-1 services to connect to, and utilize the ESInet.
- The LPG provides NG9-1-1 / SIP interface towards ESInet and a selective router based Automatic Location Identification (ALI) interface towards the PSAP.
- The LPG will not require the PSAP to upgrade to NG9-1-1 but may require the PSAP to ensure that GIS is compatible with NG9-1-1 service.
- LPG deployment may be considered a temporary measure until selective routing is discontinued.

Legacy Selective Router Gateway

The ESInet will employ a Legacy Selective Router Gateway (LSRG) at the interconnection point between the current Selective Router network provider to ensure legacy 9-1-1 calls route into the ESInet and to the PSAP.

- LSRGs will be utilized to provide tandem to tandem transfer between the selective router and the ESInet.
- The LSRG will allow calls connected to selective router to terminate on an NG capable PSAP.
- The LSRG will allow calls originating on a carrier transitioned NG9-1-1 to terminate on a legacy PSAP that is still connected to the selective router.
- The LSRG will ensure the transfer of calls among NG9-1-1 and legacy PSAPs.
- The LSRG will be removed when the last carrier and PSAP are transitioned to NG9-1-1.
- The LSRG will allow for location queries across the ALI Location Information Server (LIS) boundary.

2.15 Disaster Recovery / Business Continuity

Vendors will be required to include a method for disaster recovery and continuity of operations within the ESInet solution. The ESInet must perform all functions as specified and offer continuity of operations in the event of a malfunction of the network, system or i3 components.

The ESInet must be structured to automatically or routinely backup configuration data, and the vendor must outline the process and conditions used to restore the configuration of network elements such as routers or switches, should the need arise.

In addition to automatic, regular backups, the ESInet vendor must consider and introduce a method to perform on-demand backups, such as at the end of a successful configuration change.

All vital system components must be protected through the use of redundant modules to eliminate any single point of failure including:

- Building specific emergencies (e.g., bomb threat, power failure, tornado, hurricane, flood)
- Risks that eliminate or impede data center functionality (e.g., water, flood, power, electrical, and fire)
- Security (e.g., information and network security, physical security)
- Epidemic or pandemic factors
- Inclement weather
- Natural or man-made disasters

In the event of unplanned system or network outages, the ESInet and critical 9-1-1 systems must continue operating while mitigation and recovery processes are engaged to identify and resolve issues so that redundancy is fully restored.

Continuity plans must cover the ability to continue normal operation of the ESInet and 9-1-1 systems. The ESInet vendor will supply a continuity plan to the NMAC and ensure that the plan design protects all resources, operational and network.

The NMAC will be involved in the backup and recovery procedures and assist in the continuity of operations arrangement.

3. Bandwidth

The vendor will identify their network bandwidth for the Wide Area Network (WAN) and the Local Area Network interface (LAN). The vendor must provide bandwidth calculation for the WAN circuits to ensure that the basis for the calculation is expected volume, reliability, availability and foundational components. As bandwidth increases, the vendors must ensure that the network is capable of scaling to meet the service expectations without blocking, or limiting the overall service level.

At the LAN interface, the vendor must provide a description of how the bandwidth from the PSAP is internetworked to the core. This includes the routing of IP traffic over diverse LAN connections to the core and the size of those links.

A diagram of traffic flow between the LAN and WAN connections is necessary to provide assurance that bandwidth is calculated from the demarcation point directly to the ESInet core. In addition, the description of the diagram must detail the implementation of the interconnection between the LAN and WAN connections.

The vendor must also provide documentation and a calculation that demonstrates the bandwidth between all NG9-1-1 functional elements, text-to-911, text control centers, database access and components is sufficient to meet the demand of the NG9-1-1 solution.

3.1 Calculation of Bandwidth

The vendor may calculate the minimum bandwidth required between the NG9-1-1 Network and the PSAP(s) by multiplying the total number of workstations at each site that may receive calls by the bandwidth required per workstation calculated by the method described above. The sum of bandwidth per PSAP should also include a growth factor.

A typical method for establishing a minimum level of bandwidth is to use a measure of 2 Mbps per position, plus 2 Mbps per PSAP. Therefore a PSAP with 5 positions would be looking for about 12 Mbps of bandwidth to support NG9-1-1 calls and data.

The vendor must ensure that the calculated bandwidth and additional growth factor supports enough growth at all locations to avoid replacing major components such as core or on-site routers.

3.2 Scalability - Expansion Requirements

The overall design must allow for the ability to scale with respect to bandwidth, adding new sites and interconnection with other ESInets. This includes the ability to double bandwidth, doubling of the number of connected sites, and/or interconnections to as many as two (2) additional 9-1-1 call delivery ESInets such as ESInets in adjacent states.

The design must accommodate this level of expansion without wholesale replacement of network components, fork lift upgrades or excessive non incremental costs.

4. Internet Protocol Addressing

The IP network infrastructure must 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 address space. The use of encapsulation does not relieve the ability to monitor the operation of the IPv4 network.

4.1 Internet Protocol Routing

The vendor must implement their IP routing structure to support a dynamic IP routing protocol. The Department of Information Technology requests Open Shortest Path First (OSPF) as defined in the Internet Engineering Task Force (IETF) Request for Comments RFCs and as commonly implemented in the industry.

- All devices within the network shall be assigned static addresses.
- The IP routing protocol must 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.
- The vendor must work with the operators and service providers of all interconnected IP networks to resolve IP routing problems of the supplied service.
- The IP routing protocol must be set up to provide automatic IP rerouting in the event of a failure of any network facility or component, even if automatic rerouting is provided at another OSI Layer, such as Layer 2.
- The dynamic routing protocol must be configured to mitigate IP route instability in the network.
- Dynamic routing protocol(s) must be configured in a fashion that prevents serious loss of bandwidth due to routing table updates or other behavior that interferes with the operation of the network.
- The vendor must prepare to offer automatic rerouting and failover to an alternate route and meet the parameters within Section 2.6 (availability, reliability, 99.999).
- The vendor must provide an explanation of the IP routing protocol implementation. The narrative must include a description of the failure scenarios

and any re-routing capability designed within the system to avoid network instability.

- The IP network should provide private IPv4 address space but may need to deploy IPv6 with some carriers. The IP address scheme must allow for subnetting to ensure that the IP routing capability is mapped from end to end.
- IP address management software shall be implemented for this network

4.2 Core ESInet Provisioning

The Core ESInet provisioning must include the ability to utilize both IPv4 and IPv6 links to routers located at the sites. The primary routing may be IPv4 but the network must be able to support IPv6.

- The proposed network must be statically addressed at all major network interfaces, such as router interfaces.
- A "loopback" interface with a static IPv6 address should be assigned to each network element capable of IP administration.
- To the maximum extent possible, network monitoring and administrative functions must be conducted via the IPv6 network.
- Vendors must assign private IPv4 addresses.
- The subnet number for each site must be documented and reported to the NMAC.

4.3 Internet Protocol Version 4 Specific Functions

The vendor must 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. Vendors must list network functions, such as monitoring or administrative functions, that they can or will only perform using IPv4.

4.4 Port Fail Over

The vendors must list and describe the port fail-over scheme. A common fail-over scheme utilizes Ethernet failover; however, vendors may choose to offer a comparable solution. The failover operation must be one widely used in the industry that complies with open standards.

4.5 Network Address Translation

The 9-1-1 Board discourages the use of Network Address Translation (NAT) within the proposed IP network. NAT can present special problems for the reliable implementation of SIP and RTP streams that traverse the NAT device. If a vendor proposes NAT, they must document their ability to minimize issues with SIP, RTP and NAT and explain how they plan to mitigate issues if they arise.

Vendors must supply a network diagram with all subnet information and IP addressing. The diagram will provide details of the interconnections and routing structure across the system.

4.6 Back-to-Back User Agent Usage

Although NAT can cause issues with SIP and RTP, NAT may be implemented at points of interconnection with other IPv4 networks/address in order to resolve possible IPv4 addressing issues.

However, if SIP or RTP traffic needs to cross such boundaries, it must be handled with back-to-back user agent (B2BUA) type of session border controllers (SBCs), rather than via natively through NAT.

Back-to-Back User Agents must also be used to transport SIP and RTP between IPv6 and IPv4 networks, if required.

5. Network Monitoring

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

- IP network problems must utilize fault monitoring to detect, log and notify the NMAC.
- The vendor must provide timely notification to NMAC.
- Performance monitoring is a requirement to measure the variables that affect network performance and ensure adherence to the SLA.
- All IP manageable network hardware must support the Simple Network Management Protocol Version 3 (SNMPv3) specification for performance monitoring via standard management information base (MIB) objects.
- The monitoring solution must store information for reporting and subsequent retrieval purposes, including any requirements for accessing such features by the NMAC.

5.1 Network Operations Center

An interface to a fully functioning 24x7x365 Network Operations Center (NOC) is required. The NOC must be responsible for restoral or mitigation of incidents.

- The NOC must have a 24x7x365 trouble ticket system.
- The NOC must be designed to “follow the sun”.[1]
- The NOC must have the ability to generate, resolve and report on trouble tickets for all ESInet, network, PSAP, and application problems.
- The use of the network monitoring system does not preclude the NMAC 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.

[1] “Follow-the-sun” means that support literally follows the sun—it’s a type of global workflow in which issues can be handled by and passed between offices in different time zones to increase responsiveness and reduce delays. https://relate.zendesk.com/articles/follow-the-sun-support/; accessed 3/29/2016

- The NOC must have a 24x7 contact number accessible to authorized personnel, as determined and authorized by the NMAC.

- The NOC must have an escalation list complete with time frames for escalating trouble tickets.

5.2 Data Centers

The preference is for the location of the data centers that serve the NG9-1-1 system to be within the state of North Carolina. All potential data centers either within the State or at the vendor location may be evaluated in accordance with their functional capabilities. The following tiers represent a classification of typical data centers.

The state of North Carolina requires that all Data Centers utilized for 9-1-1 meet Tier 3 or higher criteria as defined here:

Tier 1 data center

A Tier 1 data center maintains a single path for all capacity loads. This type of data center has no redundant paths or fault tolerant infrastructure. These data centers are particularly vulnerable during an incident. In addition, this type of data center should be evaluated in terms of potential downtime per year and are characterized by having:

- Single distribution paths
- No fault tolerance
- Not decentralized
- Limited continuous heating / cooling during a utility outage
- Limited transition to emergency generator

Tier 2 data center

A Tier 2 data center can support the capacity load across multiple connections, but lack redundant paths and fault tolerance. This type of data center can remain functional for a period of time with some level of service degradation.

- Multiple distribution paths
- No fault tolerance
- Not decentralized
- Limited continuous heating / cooling during a utility outage
- Limited transition to emergency generator

Tier 3 data center

A Tier 3 data center can support the capacity load across multiple connections and does contain an additional level of redundancy.

- Alternate distribution paths
- Fault tolerance
- Decentralized
- Limited continuous heating / cooling during a utility outage
- Limited transition to emergency generator.

Tier 4 data center

A Tier 4 data center can support an outage using multiple connections. In addition this type of data center can support the capacity load during a failure without limitation.

- Simultaneously operating alternate distribution paths
- Fault tolerance
- Decentralized
- Continuous heating / cooling during a utility outage
- Immediate transition to emergency generator.

5.3 Network Configuration and Change Management

The vendors must describe their process and Standard Operating Procedure (SOP) used for making changes to the network and/or its configuration, including, at a minimum:

- Methods for planning, authorizing, authoring, reviewing, implementing, testing, back out and back up of changes

- To the extent possible, procedures for the recognition of unplanned changes that arise

- Identification of the personnel involved in the Change Management process

- Processes for changes that may include adding a connection, re-provisioning a circuit, or changing a QoS priority

- The vendor must include an automatic or routine backup of the network configuration data, such as router and switch configurations

- A description of the process and conditions used to restore the configuration of network elements such as routers or switches

- In the event of a critical or major outage, the proposer must provide the State staff with a root cause analysis within five (5) business days

- Description of the tools and techniques to perform troubleshooting and post-event analysis

5.4 Scheduled Maintenance

The ESInet vendor must include a schedule of preventive maintenance activities, including the frequency and strategy to continue network functionality during maintenance activities. The expectation is this schedule will be routinely and regularly updated and communicated to the NMAC to ensure correct preparation before the commencement of the maintenance activities.

These activities must not negatively impact the operation of the 9-1-1 service either at the ESInet core or at a PSAP. The vendor must notify the state of North Carolina NG911 Board of any scheduled maintenance activities at a minimum of 14 days in advance to ensure PSAP notification of the maintenance activity.

- The ESInet vendor must provide a notification prior to planned or scheduled maintenance.

- Any maintenance, including upgrades to the network, shall be conducted in accordance with a mutually determined and agreed upon SOP.

- The ESInet vendor must ensure that a remote location and its designated back up are not affected at the same time.

- The process must include support logs to drive the development of solutions to recurring issues.

- The ESInet vendor must test all network components within the solution and service them on a semi-annual basis at a minimum. The vendor must prepare the tests and deliver them to the NMAC prior to testing. The results of the tests will also be documented and reviewed with the NMAC once the tests have been completed.

5.5 Security Monitoring and Management

Monitoring and management services must include security monitoring and management. Monitoring of the network includes the logging of all users who attempt to access the network and resources. The management capability must allow the refusal of access to prevent inappropriate or malicious access.

The ESInet vendor must detect and prevent intrusion to the network resources, recognize and eliminate threats to the network, provide alerting, logging and reporting of security threats by intruders to the NMAC. ESInet vendors must ensure that all network resources and NG9-1-1 functional elements are configured to withstand these attacks and protect the integrity of the entire 9-1-1 system.

The monthly SLA reporting framework must include security reports.

Solutions must comply with the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security policies and practices. They are available at http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view.

Respondents shall propose how their solution meets these security measures and how they comply with future changes to security measures to ensure that:

- Network operations are not disrupted due to a security breach
- Unauthorized individuals cannot access the network
- Least access policy is applied
- Data theft does not occur
- Monthly assessments of vulnerabilities and frequent scans for malicious activity occur
- Security incidents are documented, risks identified, responded to and mitigated
- Documentation of the management of security changes
- Maintenance of security documentation to aid in forensic audits as necessary
- Maintenance of security data as recovered and not modified or deleted
- Implementation of intrusion protection and intrusion detection throughout the network to eliminate breach of security

- Protection from identify theft occurs

ESInet vendors shall include physical and logical security precautions in their proposed solution that meet the minimum criteria outlined above. This includes providing a description of any security based appliances necessary to meet the objectives including:

- Firewalls
- Access Control Lists
- Switches
- Routers
- Intrusion Protection devices
- Intrusion Detection devices
- Specialized Cabling

ESInet vendors shall provide vulnerability testing and penetration testing to ensure routine probing of the network for security holes. These tests should be performed quarterly; but may be requested by the NMAC upon the recognition of a potential vulnerability.

5.6 Encryption

The ESInet vendors must include the advanced encryption standard (AES) on their proposed solution where appropriate.

5.7 Remote Access and Network Security and Firewalls

The ESInet will include a firewall solution that provides security and protection to the system. All such interfaces connected shall be in accordance with mandated security requirements.

Secure remote access shall be strictly controlled. Control will be enforced via remote access authentication using security tokens that provide one-time password authentication or public private keys with strong pass-phrases.

The vendor’s security solution must include a method to control access to network resources to prevent sabotage and the compromise (intentional or unintentional) of sensitive information.

Remote Access control will be enforced via network and system level auditing.

5.8 Security Techniques and Protocols

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

Any LAN supplied and installed at a PSAP or other edge site to provide NG9-1-1 call delivery services or interconnect equipment is intended to be a limited access and secure LAN.

If a PSAP LAN is interconnected with other LANs at the PSAP they must also comply with the security techniques of the ESInet.

Any empty, spare or otherwise unused Ethernet ports on equipment (such as routers and switches) supplied shall be administratively disabled at the time of ESInet and NG9-1-1 service is commissioned.

Any workstations or computer equipment supplied, if equipped with Universal Serial Bus (USB) ports and/or removable media storage devices, must have such USB ports and or removable media storage devices physically or administratively disabled or otherwise restricted.

5.9 Interconnection of Other Networks

Until the completion of deployment of the NG9-1-1 system to all local PSAPs and any PSAPs that elect to participate, the ESInet’s only end purpose will be accepting 9-1-1 calls from the public and delivering those calls to the PSAPs.

However, the ESInet must be scalable and able to interconnect with other edge site LANs that connect to the PSAP for 9-1-1 related purposes. These LANs may include computer aided dispatch (CAD) systems or other Public Safety applications as may be approved by the state of North Carolina NG911 Board at any point during or after the initial project.

Any IP network authorized by the state of North Carolina 9-1-1 board to connect to the ESInet must comply with standards, including the security standards, and demonstrate compliance through an initial and recurring audit.

5.10 Anti-virus Software

The ESInet design requires at least 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.

- The anti-virus firewall must use an antivirus database that scans incoming and outgoing packets for the presence of malicious software, and blocks and logs such activities.

- The anti-virus database must be maintained and coordinated to minimize the potential of multiple databases on the same network.

5.11 Transient Voltage Surge Suppression

In addition to primary protection, copper wire connections require the installation of secondary Transient Voltage Surge Suppression (TVSS).

- Transient Voltage Surge Suppression (TVSS) devices should be used to 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 CPE and facilities.

- The installation at sites must include termination at all ground bars and ground wiring for installation at each site as required.

- The secondary TVSS devices shall list a clamping voltage of 250 volts or less and operate in less than 10 nanoseconds.

- The TVSS device shall meet UL497A requirements and must include an operational indicator to alert maintenance personnel that the device has been utilized, failed or that the circuit is unprotected.

- The secondary TVSS must not degrade the audio signaling.

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

6. NG 9-1-1 Requirements

The ESInet vendor must collaborate with the state of North Carolina to develop a plan to utilize network connections in a phased approach as PSAPs migrate to the Statewide ESInet. These requirements are determined from the State's perspective, and therefore may not specify each and every element necessary for the vendor to deliver the NG9-1-1 services.

The ESInet vendor will design, plan and implement the most effective and efficient ESInet and NG9-1-1 capable solution. The solution must include or integrate to the following functional elements necessary for NG9-1-1:

- Border control function (BCF)
- Emergency call routing function (ECRF)
- Emergency services routing proxy (ESRP)
- Legacy network gateway (LNG)
- Legacy PSAP gateway (LPG)
- Legacy selective router gateway (LSRG)
- Location validation function (LVF)
- Policy routing function (PRF)

The ESInet vendor must clearly identify where the functional elements are located, how they are addressed and configured and provide documentation including "as-built" information that describes their operation and function within the NG9-1-1 system.

The state of North Carolina 9-1-1 Board recognizes that all of the functions listed above may not be required at the initial development and deployment stage. As the ESInet network and NG9-1-1 system evolves, more of the functional elements may be required to support NG9-1-1 call delivery throughout the State. Figure 4 provides a functional NG9-1-1 framework diagram.

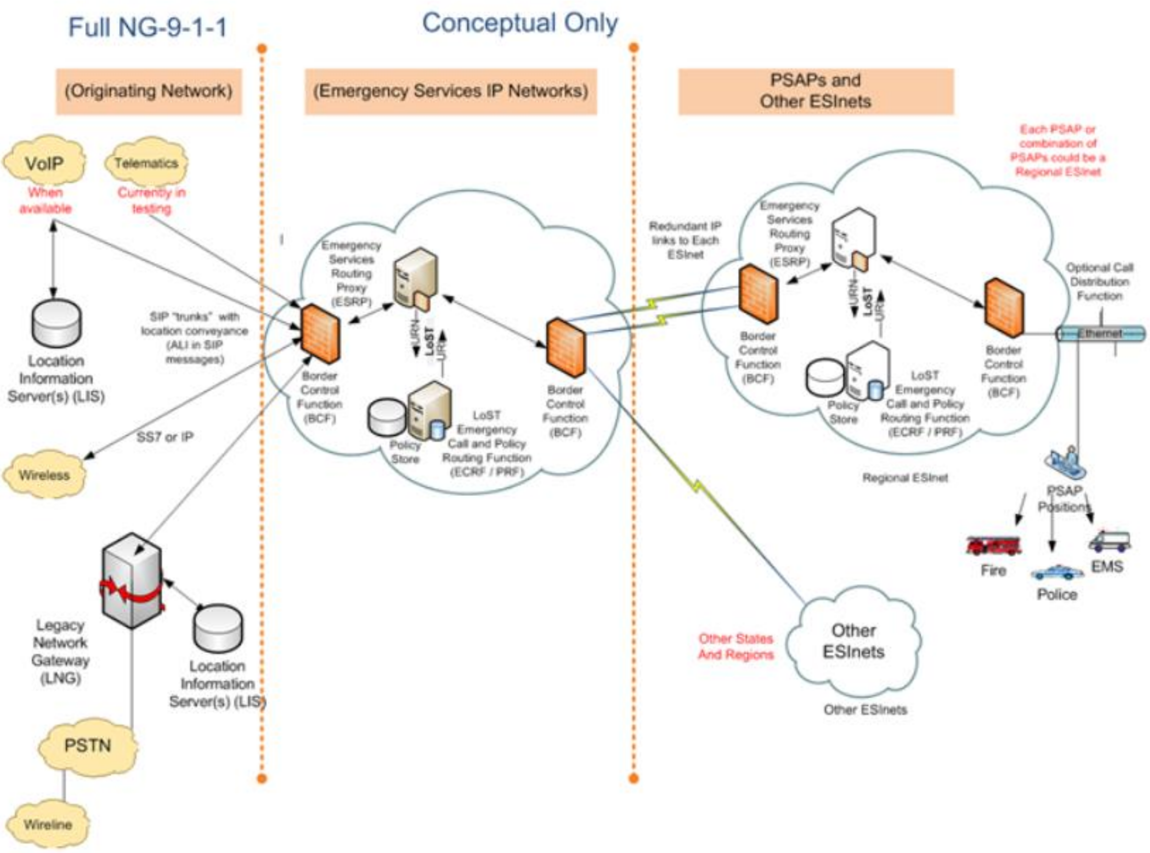
Full NG-9-1-1
Conceptual Only
(Originating Network)
(Emergency Services IP Networks)
PSAPs and Other ESInets
VoIP
When available
Telematics
Currently in testing
Location Information Server(s) (LIS)
SIP "trunks" with location conveyance (ALI in SIP messages)
SS7 or IP
Wireless
Legacy Network Gateway (LNG)
Location Information Server(s) (LIS)
PSTN
Wireline
Emergency Services Routing Proxy (ESRP)
URN
LoST
URI
Border Control Function (BCF)
Policy Store
LoST Emergency Call and Policy Routing Function (ECRF / PRF)
Border Control Function (BCF)
Redundant IP links to Each ESInet
Emergency Services Routing Proxy (ESRP)
URN
LoST
URI
Border Control Function (BCF)
Policy Store
LoST Emergency Call and Policy Routing Function (ECRF / PRF)
Border Control Function (BCF)
Each PSAP or combination of PSAPs could be a Regional ESInet
Optional Call Distribution Function
Ethernet
Regional ESInet
PSAP Positions
Fire
Police
EMS
Other States And Regions
Other ESInets
Other ESInets

Figure 4 – Functional NG9-1-1 framework

6.1 Border Control Function (BCF)

Per the NENA i3 NG9-1-1 specification, the network must be configured with a Border Control Function (BCF).

The BCF supports a variety of direct IP interconnection arrangements between the ESInet and external IP networks depending on the level of mutual trust that exists between the respective networks. The preference is the location of BCFs at a minimum of two geographically diverse points of interconnection on the network, and support 99.999 availability and reliability. The BCF will support:

- External security border for ESInet
- Internal isolation border for PSAP
- Both firewall and Session Border Controller (SIP specific) parts
- Ability to mark calls with suspicion levels
- Functions to block specific call sources

- ESInet BCF must withstand largest feasible attack (currently in the range of 10G)

6.2 Distributed Denial of Service (DDoS attack prevention)

ESInet plans and designs should take into consideration a DDoS mitigation service in addition to utilizing the BCF for that function. A DDoS attack could interfere with an ESInet by attacking the Domain Name Server (DNS), attacking a specific protocol or through packet flooding. The ESInet vendor must provide a method of avoiding these potential vulnerabilities.

The ESInet vendor may provide a separate BGP route that can be withdrawn to eliminate the infected route, and replace it with a route to the mitigation service. Where DNS is not provided in the same route, separate arrangements may be necessary for DNS service.

Depending on the configuration of the external ECRF/LVF, the paths to that ECRF may also be exposed to DDoS outside of an ESInet and require additional protection.

DDoS mitigation considerations for public addressing:

- There must be an external ECRF and an external LVF. These could be in an ESInet Demilitarized Zone (DMZ), or on a completely separate public network. The external ECRF and LVF must have global DNS entries.

- NENA i3 08-003 states that PSAPs must provide public addressable endpoints for media to avoid the need for NAT traversal gyrations. The BCF must provide media anchoring to supply the global media addresses.

- The entrance ESRP and/or the BCF which is the target of the URL in the external ECRF for PSAPs inside an ESInet must be publicly addressable and its entry (the domain in the URL found in the ECRF) must be in the global DNS.

- An LIS may provide a "Presence" URL for location by reference using a SIP SUBSCRIBE/NOTIFY. Any entity that wishes to dereference such a URL requires a public address, and typically a global DNS entry. The list of such dereferencers includes all ESRPs, all PSAPs, all responders, etc.

- A call may include additional data about a call, caller, or location. That information may be sent by reference, requiring access from an entity inside an ESInet to the external Additional Data Repository (ADR) or Identity Searchable Additional Data Repository (IS-ADR). PSAPs, responders and other agencies may need this information. It is possible for a Policy Routing Rule to use such data, and thus all ESRPs may need to query. In these cases, the query is HTTPS, and could be through a NAT.

- There are circumstances where 9-1-1 Authorities may provide a provisioning feed to an ECRF or LVF maintained by some outside entity such as a service provider. The feed might be provided by the external ECRF/LVF, but if it is not, the Spatial Interface (SI) for such a feed needs a global address and global DNS entry.

- There are circumstances where an agency may wish to provide an Emergency Incident Data Document (EIDD) feed to an external entity. If that is permitted, the entity providing the EIDDs must be publicly addressable. It is possible the feed is a subscription, in which case the EIDD source needs a global DNS entry.

6.3 Emergency Call Routing Function (ECRF)

In the process of delivering a 9-1-1 call, an origination network may use an Emergency Call Routing Function (ECRF), or a similar function within its own network, to determine an appropriate route to a PSAP or another ESInet.

ESInet vendors must be prepared for providing an ECRF and ensuring that it is accessible from outside the ESInet. The ECRF must permit querying by another ECRF or router, a Legacy Network Gateway (LNG), or an Emergency Services Routing Proxy (ESRP).

The ECRF and the interconnection must be designed according to NENA i3 standards and be implemented using diverse, reliable and secure IP connections.

- ECRF functions must meet a minimum of 99.999 availability and reliability.

- An ECRF accessible inside an ESInet must permit querying from any entity inside the ESInet.

- An ECRF must support a routing query interface that an endpoint, ESRP, or PSAP can use to request location-based routing information from the ECRF.

- An ECRF must interface with the Location to Service Translation (LoST) protocol (RFC5222) and support LoST queries via the ESRP, PSAP customer premise equipment (CPE), or any other permitted IP host.

- An ECRF must allow for rate limiting queries from sources other than the proposed ESRP(s), and provide logging of all connections, connection attempts, and LoST transactions.

- An ECRF design and implementation must support the ability for GIS data management functions to ensure maintenance of accurate location data.

The ECRF must also support:

- Correction of location errors
- Route calls based on geographical coordinates and civic addresses
- Utilize common GIS boundaries (Municipal, Police, Fire, EMS)
- Permit LoST association with each layer
- Comply with NENA i3 and NENA STA-014
- Support dynamic updates to GIS without disruption of the ECRF
- Validate GIS updates before they are applied

GIS information is the primary data used by the ECRF to route 9-1-1 calls. ESInet vendors must explain their method for collecting GIS information and establishing that the GIS information is valid for use with the ECRF. Vendors must explain where the ECRF is located and how it will operate, including:

- How the proposed ECRF and its capabilities, features, functions and protocols provide high reliability routing for all 9-1-1 call types

- The interface to the ECRF that provides the ability to upload location information once the Extensible Markup Language (XML) is published and approved for general use

6.4 Emergency Services Routing Proxy (ESRP)

ESInet vendors must include an Emergency Service Routing Proxy (ESRP) for call delivery to the appropriate PSAP based upon location and routing rules. Vendors must provide an explanation of the ESRP and identify the location of the ESRP. Vendors are responsible for how the ESRP operates within their proposed solution including:

- Carrier to ESRP
- ESRP to ERSP
- ESRP to call-taker routing

The configuration of vendors' ESRPs must comply with NENA i3 specifications and provide the ability of the ESRP to route SIP messages to a PSAP. Vendors must also document how the ESRP interfaces to the ECRF and to the Policy Routing Function

(PRF) to ensure that routing instructions, routing policies and possible event notifications that alter call routing scenarios are appropriate.

Per NENA i3 for typical 9-1-1 calls received by an ESRP, it:

- Evaluates a policy "rule set" for the queue the call arrives on
- Queries the location-based routing function (ECRF) with the location included with the call to determine the "normal" next hop (smaller political or network subdivision, PSAP or call taker group) Uniform Resource Identifier (URI).
- Evaluate a policy rule set for that URI using other inputs available to it such as headers in the SIP message, time of day, and PSAP state.

The result of the policy rule evaluation is a URI. The ESRP forwards the call to the URI.

6.5 Policy Routing Function (PRF)

The Policy Routing Function (PRF) is the primary routing component of the ESRP. The ESRP uses defined routing policies within the ESInet and the NENA i3 network to deliver calls to the proper PSAP. The PRF function itself requires an ESRP to assist in the dynamic call routing and re-routing based upon other policy rules beyond normal operation.

ESInet vendors must provide a detailed description of how the PRF will operate within the NG9-1-1 solution and explain the method of implementing custom policies. Vendors must also describe any interfaces used to modify polices to ensure that the PRF functions as needed.

6.6 Legacy Network Gateway (LNG)

The Legacy Network Gateway (LNG) is a gateway located between the legacy 9-1-1 network and the ESInet. An LNG allows NG9-1-1 capable PSAPs to receive emergency calls from legacy originating networks. The state of North Carolina recognizes that LNGs are necessary during transition to NG9-1-1. LNGs are typically necessary at all PSAPs that are ready for NG9-1-1 that rely on a legacy 9-1-1 network for call origination. The expectation in that LNGs will facilitate a more efficient migration.

9-1-1 calls originating in legacy networks will use the LNG to convert the incoming Multi Frequency (MF) or Signaling System Number 7 (SS7) signaling to the IP-based signaling supported by the ESInet. Thus, the LNG supports a physical SS7 or MF interface on the side of the legacy 9-1-1 network, and an IP interface which produces SIP signaling towards the ESInet.

- The LNG implementation must correctly route emergency calls to the appropriate ESRP in the ESInet.
- The LNG must use the location information to query an ECRF and obtain routing information in the form of a URI.
- The LNG must forward the call or session request to an ESRP in the ESInet, using the URI provided by the ECRF, and include callback and location information in the outgoing signaling.
- The LNG must be capable of appending supplemental and supportive call information such as location and callback number to the call prior to the ESInet.

Vendors must indicate how the legacy network gateway (LNG) function is configured to integrate the legacy network with the core ESInet and NG9-1-1 system.

6.7 Legacy PSAP Gateway (LPG)

The legacy PSAP gateway (LPG) provides a seamless connection to PSAPs not upgraded to NG9-1-1 PSAP operations. The LPG is a signaling and media interconnection point between an ESInet and a legacy PSAP that allows for the delivery of 9-1-1 calls that traverse an i3 ESInet to get to a legacy PSAP.

An LPG supports an IP (i.e., SIP) interface towards the ESInet on one side, and a traditional MF or Enhanced MF interface (comparable to the interface between a traditional Selective Router and a legacy PSAP) on the other. In addition the LPG supports:

- An ALI interface which can accept an ALI query from the legacy PSAP
- Generation of a response with location information, formatted according to the ALI interface supported by the PSAP

6.8 Legacy Selective Router Gateway (LSRG)

The primary function of a Legacy Selective Router Gateway (LSRG) is to allow traffic from legacy Selective Router based networks to ESInets. The LSRG must serve as the interface for legacy selective routers to terminate trunks utilizing an inter-tandem trunk group method of termination.

The LSRG converts a 9-1-1 call signaling to SIP/RTP then queries the existing ALI data management system to retrieve location information for the call. Following retrieval of the data to route the 9-1-1 call, the LSRG routes the 9-1-1 call to the next nominal hop based on a LoST query to an ECRF. The LSRG must include the ability to facilitate bi-directional communications with the legacy selective routers for both voice and data (star codes) transactions.

6.9 Location Validation Function (LVF)

The Location Validation Function (LVF) in NG9-1-1 systems generally only performs the function of verifying civic (street address) location. The LVF utilizes the Location Information Server (LIS) to determine the geographical location of a 9-1-1 call. The LVF design must rapidly determine the validity of an address and respond.

The LVF data and interfaces are similar to those used by an ECRF representing the same geographic area(s).

Vendors must describe their proposed LVF implementation, with particular attention to the arrangement of the proposed components, user interface and features, and the security aspects of the LVF.

6.10 Location Information Services (LIS)

9-1-1 caller location is fundamental to the operation of the NG9-1-1 system. Location provision is external to the ESInet, and the functional entity which provides location is a Location Information Server (LIS). While the LIS is an external database, the vendor must supply an interface from the network to the LIS. ESInet vendors must include the necessary security provisions described earlier on any interface and provide a description of the communication paths between the LIS and the LVF, LSRG and LNG.

6.11 ALI Database Services

The state of North Carolina NG911 Board recognizes the requirement of ALI database services for the foreseeable future. ESInet vendors must include details about their approach to ALI database connections and ALI maintenance functions that will be necessary for the short term during deployment of NG9-1-1 functionality. The vendor must continue to operate, manage and maintain the proposed ALI database service and consider PS/ALI capabilities where necessary.

6.12 Text to 9-1-1 requirements

North Carolina NG9-1-1 requires a text solution that is in compliance with the Alliance for Telecommunications Industry Solutions (ATIS) / Telecommunication Industry Association (TIA) J STD 110, Joint ATIS/TIA Native SMS to 9-1-1 Requirements & Architecture Specification A J STD 110 Standard.

The state of North Carolina NG911 Board seeks a text-to-9-1-1 emergency telecommunications system that integrates with their current model already in use at the PSAPs. The current method is utilization of the TTY system for delivering text messages to the PSAP. The goal is for implementation of the NG9-1-1 network to provide the ability for a Text Control Center (TCC) model. However, the NG9-1-1 system must continue to support the current model of Text over TTY.

Functionally, the state of North Carolina NG911 Board's preference is to have emergency text messages (text-to-9-1-1) from all wireless carriers aggregated and delivered through a Message Session Relay Protocol (MSRP) implementation. The MSRP solution is an IETF standard framework documented in RFC 4975. MSRP ensures the delivery of all messages via a Session Initiation Protocol (SIP) framework and through the CPE solution. The MSRP standard utilizes the NG9-1-1 network to allow instant messaging between a caller and an operator using a standard interface.

The state of North Carolina NG911 Board will require vendors of text-to-911 to implement a solution that includes an MSRP integration and NENA STA-010 compliance with direct connectivity to the CPE. MSRP integration will aid in optimizing the PSAP NG9-1-1 transition by allowing text messages to utilize the same interface as voice calls. In addition the MSRP method allows for text-to-911 transcripts to be collected as a part of the call detail record for logging and reporting.

The system design must only require that a person requiring emergency assistance enter the short code "9-1-1" in their wireless device in order to have an emergency text message sent to a PSAP and not utilize a separate application or other text messaging service or solution.

The text-to-911 service should not contain any other type of code to reach a PSAP nor should an application be necessary on a mobile device. Likewise, a person should not need to register their device in order to text 9-1-1 within the North Carolina.

In addition the text-to-911 solution must allow the transfer of messages between adjoining PSAPs (primary and secondary) that use a web-based browser or NENA i3 CPE interfaces.

Vendors of the text-to-911 solution must provide an aggregation function that:

- Will aggregate text-to-9-1-1 messages from multiple TCCs into a single message stream for distribution to the PSAPs
- Supports any Alliance for Telecommunications Industry Solutions (ATIS) compliant text-enabled CPE interface
- Supports transfer of text sessions between different interfaces

Vendors must also provide a Distributor function that:

- Receives text-to-9-1-1 messages from the Aggregator and uses the ESRP/ECRF to route the message to the destination PSAP for the PSAPs served by the Distribution server.
- The Distributor includes:
    - SIP/MSRP Interface - interface between the Aggregator and the NENA i3 ESInets or MSRP CPE at the PSAP and will require integration into the CAD system

Appendix A - Applicable Global Standards

The North Carolina NG9-1-1 implementation requires adherence to the following standards listed here in no particular order of preference or priority:

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 ANSI/EIA/TIA-568 Commercial Building Telecommunications Wiring Standards), etc.

NENA i3 standards

NC ESInet and NG9-1-1 requires adherence to standards found in these documents:

NENA Detailed Functional and Interface Standards for NENA (i3) Solution Stage 3 08-003

NENA Security for Next-Generation 9-1-1 Standard (NG-SEC, document 75-001 dated February 6, 2010)

Next Generation 9-1-1 Security (NG-SEC) Audit Checklist NENA 75-502 V1

NENA i3 Technical Requirements Document 08-751

FBI Criminal Justice Information Services (CJIS) Security Policies

http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view

Security in the ESInet must be in accordance with the requirements above and any additional security policy determined to be a standard utilized by the Department of Information Technology. The State may modify this list of approved standard policies at any time at its sole discretion.

Appendix B - Applicable Documents

The following list consists of documents relevant to this conceptual design:

NENA ADM-000 - Master Glossary of 9-1-1 Terminology

NENA 08-003 v1 - NENA Functional and Interface Standards for Next Generation 9-1-1 (i3)

NENA 75-001 v1 - NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)

NENA Baseline Next Generation 911 Description, February 22, 2011

National Institute of Standards and Technology (NIST) 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations

RFC 3261 - SIP: Session Initiation Protocol

RFC 3376 -Internet Group Management Protocol, Version 3

RFC 4604 - Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast

RFC 3973 - Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)

RFC 5015 -Bidirectional Protocol Independent Multicast (BIDIR-PIM)

RFC 3569 - An Overview of Source-Specific Multicast (SSM)

RFC 4601 - Protocol Independent Multicast - Spare Mode (PIM-SM): Protocol Specification (Revised)

RFC 2328 - OSPF Version 2

RFC 4271 - A Border Gateway Protocol 4 (BGP-4)

RFC 3411 - An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

RFC 3412 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) Management Frameworks

RFC 3413 - Simple Network Management Protocol (SNMP) Applications

RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

RFC 3415 - View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

RFC 3416 - Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)

RFC 3417 - Transport Mappings for the Simple Network Management Protocol (SNMP)

RFC 3418 - Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)