Develop a set of requirements for the ESI Net using existing resources as a source. These requirements will later be validated with the user community through regional work sessions.

Industry Standards

The ESInet should adhere to industry standards; most notably for technical standards is NENA 08-003, *Detailed Functional and Interface Standards for Next Generation 9-1-1, Version 1.0 (i3),* and NENA INF-008.2-2013, *NENA NG9-1-1 Transition Plan Considerations Information Document*.

Additionally, the ESInet should conform to all FCC rules.

High-Level Design Requirements

The ESInet should satisfy these high-level design 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
- 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.
- ESInet infrastructure should be an open-standards-based

Originating Call Network and Ingress to the ESInet

Some of the first questions related to ESInet design involve calls entering the network. How do communications service providers (CSPs) interface with the ESInet? The ESInet will receive calls from wireless carriers, wireline carriers, and VOIP & telematics providers. Does the Commonwealth want the CSPs to connect directly to the ESInet, and how would the CSP's be compelled to do so?

Currently there are 18 selective routers across Virginia. During the migration away from the selective routers, there could be up to 24 new points of interface (POIs) for carriers to deliver traffic. (12 LATAs in Virginia that could require 2 POIs each). It would be costly for the Commonwealth to provision facilities at 24 POI's. Conversely the Commonwealth could choose to provision only 2 geographically diverse POI's, but then existing CSPs would need to install expensive long-haul circuits from all across the state.

The challenge in designing the ingress network will be finding a reasonable and efficient manner for asking the carriers to deliver their traffic. Reasonable and efficient being considered as the Commonwealth providing LNGs in the closest proximity to the highest concentration of originating switches with the fewest number of LNGs as possible.

Statewide Core Services - based on cost and needs of PSAPs

As part of the statewide ESInet backbone, consensus should be reached on what core services or functions would be provided by the Commonwealth. Some of the most likely elements are:

- Border Control Functions – Firewalls between the CSPs, PSAPs, regional ESInets and the State ESInet.
- Emergency Services Routing Proxy / Policy Routing / Policy Store – Were call information is processes and delivered.
- Geographic Information System Services – A GIS database used by the ECRF to route calls to the most appropriate PSAP.
- Location Validation Function – A means where authorities can pre-verify that an address is in the correct format, is valid in the GIS database, and returns appropriate PSAP & first responder information to that location.
- Emergency Call Routing Function – Use to route an emergency call to the appropriate PSAP for the callers location.
- Legacy Network Gateway – An interconnection between the legacy wireless/wireline networks and the ESInet.

Open Systems Interconnection model (OSI Model) layers

The options for the foundation of the network are as follows:

Layer 1 – Physical: Options for this layer include copper, fiber, or microwave. The recommendation by MCP is that fiber be the first choice where feasible.

Layer 2 – Data Link: Options for this layer include MPLS, Ethernet, HDLC and ATM. The recommendation by MCP is that Ethernet is the preferred technology.

Layer 3 – Network: IP addressing, routing and switching. Recommendation is that both IPv4 and IPv6 are to be supported.

Managed Network Services

The ESInet will require several applications that either are directly part of it, or support it. An entity will need to be in charge of providing the following services:

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

Monitoring

It is critical that the ESInet be monitored at all times. The entity in charge of monitoring the ESInet should be required to provide:

- A 24/7/365 NOC
- Levels 1, 2, and 3 technical support
- A service portal for opening trouble tickets, and checking status of existing tickets
- Statistics including, but not limited to, uptime, latency, jitter, packet loss, bandwidth utilization, and Mean Opinion Score (MOS)
- Documented escalation procedures
- Documented change management procedures
- Monthly trouble reports showing tickets opened, resolved, and unresolved
- Regular change reports showing changes requested, approved, completed, in progress, and failed/backed out
- RFO/post-mortem within a reasonable time

Network Diversity & Availability

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. Where economically available, the network Core solution and redundantly connected End Sites shall include physically diverse routes and physically diverse building entrances. Any network elements that are not provisioned with physical diversity need to be clearly identified.

With 121 PSAPs in the Commonwealth, there may be instances where diversity is not always economically reasonable. The general assumption would be that some of the smaller PSAPs would have fewer options for physical connectivity, or much higher costs for the provisioning of facilities that would

require trenching in new circuits. A test based on the cost of the new facilities, size of the PSAP, and the population served should be developed to determine the economic reasonableness for network diversity to individual PSAPs.

At fully redundant end sites, the ESInet should be designed to provide 99.999% availability to all sites as measured monthly.

Network Security Recommendations

The ESI net should have an infrastructure that protects the confidentiality of communications, provides resistance to tampering, supports effective management, and supports unique addressing of any device or endpoint. The ESInet should be implemented with the following characteristics

- Use of IPv6 addressing throughout with IPSec security enabled
- Implementation of Secure Domain Name Services (DNSSEC) within the network(s)
- Redundant, diverse Network Time Servers, with each network device using Network Time Protocol (NTP) directed to at least 2 reference servers.
- Simple Network Management Protocol, Version 3 (SNMPv3) with appropriate security protocols engaged
- Assignment of all entity names via fixed DHCP references (Dynamic Host Configuration Protocol)
- Use of Dynamic DNS, sourced to the DHCP Servers
- Establishment of an internal Public Key Infrastructure (PKI) certificate authority, potentially referenced to a Statewide PKI Registration authority.

Initial Core Bandwidth and Utilization

A determination needs to be made for the bandwidth of the initial core network. MCP suggests that the starting capacity of the State ring be between 1GB and 10GB. Standards would also need to be set for utilization. What would be the utilization triggers that require increases in network capacity?

Initial Physical Connections

Where will the initial physical interconnections be? Likely lists of candidates are the VITA datacenters at CESC & SWESC, additional datacenters as recommended by MCP, and all 121 primary PSAPS, LECs, and 9-1-1 service providers. But that list could also include secondary PSAPs, Virginia State Police, Fire, EMS and other public safety related entities.

Other Considerations

How do you allow the PSAP to connect the call delivery (ESI Net) to their own LAN (CAD, other applications)?

Who will migrate existing 9-1-1 services? And ensure quality and reliability?