Table of Contents

Return to Index

Table of Figures

Return to Index

Table of Tables

Return to Index

4. Technical Specifications

4.0 Background

This section describes information that will be of interest to any Respondent in the preparation of their response.

4.0.1 Acronyms and Definitions

911 Malicious Content (NMC): Malicious Content: Software or code intended to disrupt service, alter or remove information from its original location without authorization.

Access Control List (ACL): A table that specifies to a computer operating system or network device, e.g., IP router, the access rights allowed, denied, or audited for each user to a particular system object, such as a file directory, individual file, or IP address. Each system object has a security attribute that identifies its ACL. The most common privileges include the ability to read, write, and/or execute file(s), or communicate with specific IP addresses.

Adaptive Multi-Rate (AMR): An audio data compression scheme, which allows more storage on voice files, optimized for speech coding. AMR is widely used in Global System of Mobile (GSM) communication technology and uses link adaptation to select from one of eight different bit rates based on link conditions.

Adaptive Multi-Rate Wideband (AMR-WB): A speech coding standard developed based on AMR encoding. AMR-WB provides improved speech quality due to a wider speech bandwidth of 50–7000 Hz compared to narrowband speech coders, which are generally optimized for plain old telephone system wireline quality of 300–3400 Hz. AMR-WB is codified as G.722.2.

Alliance for Telecommunications Industry Solutions (ATIS): A U.S.-based organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. (NENA)

American National Standards Institute (ANSI): ANSI a private non-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the U.S.

ANI/ALI controller: A legacy 9-1-1 system component, typically located at the PSAP, which provides ANI/ALI information to the call taker answering position.

Automatic Location Identification (ALI): The automatic display at the PSAP of the caller's telephone number, the address/location of the telephone and supplementary emergency services information of the location from which a call originates. (NENA)

Automatic Number Identification (ANI): Telephone number associated with the access line from which a call originates. (NENA)

Back to Back User Agent (B2BUA): (SIP) A logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request should be answered, it acts as a user agent client (UAC)

and generates requests. Unlike a proxy server, it maintains dialog state and must participate in all requests sent on the dialogs it established. (NENA)

Bidirectional Forwarding Detection (BFD): A detection protocol designed to provide fast failure detection times for all media types, encapsulations, topologies, and routing protocols. BFD can detect failures, but the routing protocol must take action to bypass a failed peer. BFD is UDP-based and provides fast routing protocol independent detection of layer-3 next hop failures. BFD provides low-overhead detection of faults even on interfaces that do not support failure detection of any kind, such as Ethernet, virtual circuits, tunnels and MPLS paths. (Cisco)

Border Control Function (BCF): Provides a secure entry into the ESInet for emergency calls presented to the network. The BCF incorporates firewall, admission control, and may include anchoring of session and media as well as other security mechanisms to prevent deliberate or malicious attacks on PSAPs or other entities connected to the ESInet. (NENA)

Border Gateway Protocol (BGP): An IETF standard, and the most scalable of all routing protocols, BGP backs the core routing decisions on the Internet. BGP maintains a table of IP networks that designate network reach-ability among autonomous systems. BGP makes routing decisions based on path, network policies and/or rule-sets. BGP can carry routes for Multicast, IPv6, VPNs, and a variety of other data.

Building Industry Consulting Service International, Inc. (BISCI): BICSI is a professional association supporting the information technology systems (ITS) industry, providing information, education and knowledge assessment for individuals and companies in the ITS industry.

Centralized Automatic Message Accounting (CAMA): A type of in-band analog transmission protocol that transmits telephone number via multi-frequency encoding. Originally designed for billing purposes. (NENA)

Class of Service (CoS): A designation of the type of telephone service, e.g. residential, business, centrex, coin, PBX, wireless. (NENA)

Coder/Decoder (CODEC): In communication engineering, the term codec is used in reference to integrated circuits, or chips, [or software] that perform data conversion. In this context, the term in an acronym for "coder/decoder." This type codec combines analog-to-digital conversion and digital-to-analog conversion functions in a single chip. In personal and business computing applications, the most common use for such a device is in a modem. (NENA)

Command Line Interface (CLI): A user interface to a computer's operating system or an application in which the user responds to a textual prompt by typing in a command on a specified line, receives a response back from the system, and then enters another command, and so on.

Commercial Mobile Radio Service (CMRS): A regulatory classification for mobile telephone service created by the FCC in response to the Omnibus Budget Reconciliation Act of 1993.

Commercial Off-the-Shelf (COTS): A non-developmental item of supply that is sold in substantial quantities in the commercial marketplace that can and is procured by the general public, as opposed to purpose-built/developed, limited production specialty items. Examples of COTS hardware and software (in the context of this document) are IP routers, Ethernet switches, rack-mounted server hardware, network monitoring software,

and GIS software systems.

Computer Emergency Response Team (CERT): A group of computer experts who respond to computer security events.

Configuration Management Database (CMDB): A database that contains all relevant information about the components of the information system used in an organization's IT services and the relationships between those components. CMDB provides an organized view of data and a means of examining that data from any desired perspective. (ITIL)

Continuity of Operations Plan (COOP): A plan that details how essential functions of an agency will be handled during any emergency or situation that may disrupt normal operations.

Customer Premise Equipment (CPE): Communications or terminal equipment located in the customer's facilities – Terminal equipment at a PSAP. (NENA)

Data Center: Any site housing equipment that is executing software that provides critical NG-911 Routing Service functions.

Demilitarized Zone (DMZ): A partially protected zone on a network, which is not exposed to the full Internet and not fully behind the firewall. DMZ is a host computer or network inserted as a neutral zone between two other computer networks. (Newton)

Denial of Service (DoS): DOS occurs when a system is overwhelmed by spurious or malicious messages in such a way that legitimate messages cannot be processed, or legitimate messages are processed extremely slowly.

Dense Wavelength Division Multiplexing (DWDN): Technology that puts data from different sources together on an optical fiber, with each signal carried at the same time on its own separate light wavelength. Using DWDM, many separate wavelengths or channels of data can be multiplexed into a lightstream transmitted on a single optical fiber. Each channel carries a time division multiplexed (TDM) signal. In a DWDM system capable of 80 channels with each channel carrying 2.5 Gbps, up to 200 billion bits can be delivered a second by the optical fiber.

Department of Management Services (DMS): The State of Florida government agency charged with human resource management, specialized services, state purchasing, and technology, among other responsibilities.

Department: The Florida DMS entities involved in the NG-911 Routing Service, including the Division of Telecommunications (DivTel), the Bureau of Public Safety, and the 911 Office.

Differentiated Services: Differentiated Services give different treatment to traffic based on the EXP bits in the MPLS label header and provide the ability for multiple classes of service.

Diffserv-aware Traffic Engineering (DS-TE): DS-TE provides traffic engineering at a per-class level rather than at an aggregate level; different bandwidth constraints for different class types (traffic classes), and different queuing behaviors per class, allowing the router to forward traffic based on the class type, making it possible to guarantee service and bandwidth across an MPLS network. (Juniper)

Digital Signal, Level 0 (DS-0): A voice-grade channel of 64 Kbps. There are 24 DS-0 channels in a T-1.

Digital Signal, Level 1 (DS1): 1.544 Mbps – symmetrical. DS1 was developed to increase the number of voice grade interoffice trunks that could function over a single twisted pair of wires. (Newton)

Digital Signal, Level 3 (DS-3): DS-3 is the equivalent of 28 T-1 channels, each operating at a total signal rate of 1.544 Mbps.

Digital Subscriber Line (DSL): A "last mile" solution that uses existing telephony infrastructure to deliver high speed broadband access. DSL standards are administered by the DSL Forum (http://dslforum.org/). (NENA)

Distributed Denial of Service (DDoS): A DDoS attack is one in which a multitude of compromised systems attack a single target, causing a denial of service for users of the targeted system. The incoming messages flood the target system, forcing it to shut down, hence denying service to legitimate users.

Domain Name Server (DNS): Used in the Internet today to resolve domain names. The input to a DNS is a domain name (e.g., telcordia.com); the response is the IP address of the domain. The DNS allows people to use easy to remember text-based addresses and the DNS translates the text into routable IP addresses.

Dual Tone Multi-Frequency (DTMF): The transmission of a selected number or symbol (*, ##) via the generation of a specific pair of tones when that number's or symbol's button on a push button telephone is pressed. Also known as Touch-Tone™. The tones are audible and transmitted within the voice band. (NENA)

Dynamic Host Configuration Protocol (DHCP): A widely used configuration protocol that allows a host to acquire configuration information from a visited network and, in particular, an IP address. (NENA)

Emergency Call Originating Network (ECON): The network of the call origination provider that is used to process and deliver 911 calls to the 911 provider's network.

Emergency Call Routing Function (ECRF): Receives location information (either civic address or geo-coordinates) as input and uses this information to provide a URI that can be used to route an emergency call toward the appropriate PSAP for the caller's location. Depending on the identity and credentials of the entity requesting the routing information, the response may identify the PSAP, or an Emergency Services Routing Proxy (ESRP) that acts on behalf of the PSAP to provide final routing to the PSAP itself. The same database that is used to route a call to the correct PSAP may also be used to subsequently route the call to the correct responder, e.g., to support selective transfer capabilities. (NENA)

Emergency Data eXchange Language – Distribution Element (EDXL-DE): EDXL-DE facilitates emergency information sharing and data exchange across local, regional, tribal, national, and international organizations in the public and private sectors. EDXL-DE acts as a wrapper that identifies to whom and under what circumstances emergency information is to be sent. Payloads may include a wide range of data types including geographic coordinates, text documents, and audio, video, and image files. Adoption of EDXL-DE as a standard by government agencies promotes emergency data interoperability among software and hardware systems, increasing the efficiency with which emergency managers receive information.

Emergency Services IP Network (ESInet): An IP-based inter-network (network of networks) shared by all agencies which may be involved in any emergency. (NENA)

Emergency Services Routing Key (ESRK): Either a 10-digit North American Numbering plan or non-NANPA number that uniquely identifies a wireless emergency call, is used to route the call through the network, and used to retrieve the associated ALI data. These numbers can be dialable or non-dialable. (NENA)

Emergency Services Routing Proxy (ESRP): An i3 functional element which is a SIP proxy server that selects the next hop routing within the ESInet based on location and policy. There is an ESRP on the edge of the ESInet. There is usually an ESRP at the entrance to an NG9-1-1 PSAP. There may be one or more intermediate ESRPs between them. (NENA)

Enhanced 911 (E-911): A telephone system which includes network switching, data base and Public Safety Answering Point premise elements capable of providing automatic location identification data, selective routing, selective transfer, fixed transfer, and a call back number. The term also includes any enhanced 9-1-1 service so designated by the Federal Communications Commission in its Report and Order in EC Docket Nos. 04-36 and 05-196, or any successor proceeding. (NENA)

Enhanced MF (E-MF): A type of in-band signaling analog trunks that use CAMA signaling protocol to out-pulse the 911 caller's ANI or pANI to the PSAP. Early MF trunks, capable of 8-digit ANI, were enhanced to provide 10 to 20 digit ANI information to the PSAP.

Enhanced Variable Rate Codec (EVRC): A voice coder used in CDMA networks. EVRC digitizes and compresses each 20 milliseconds of 8000 Hz, 16-bit sampled speech input into output frames of one of three different sizes through an EVRC digital signal processor, improving CDMA bandwidth utilization. (Newton)

Enhanced Variable Rate Codec B (EVRC-B): EVRC-B is an enhancement to EVRC and compresses each 20 milliseconds of 8000 Hz, 16-bit sampled speech input into output frames of one of the four different sizes.

Enhanced Variable Rate Codec Narrowband-Wideband (EVRC-NW): Voice coder that uses different combinations of several kinds of frame rates according to specific conditions in order to lower the average data rate.

Enhanced Variable Rate Codec Wideband (EVRC-WB): A wideband extension of EVRC-B, EVRC-WB provides speech quality that exceeds regular wireline telephony. EVRC-WB splits the speech spectrum into low frequency and high frequency bands and compresses them separately. Low frequency signal is coded based on the EVRC-B standard; high frequency signal coding is based on a LPC scheme. Principal applications of EVRC-WB include wideband telephony, video telephony, gaming, streaming, and ring-back tones.

Extensible Markup Language (XML): An internet specification for web documents that enables tags to be used that provide functionality beyond that in Hyper Text Markup Language (HTML). Its reference is its ability to allow information of indeterminate length to be transmitted to a PSAP call taker or dispatcher versus the current restriction that requires information to fit the parameters of pre-defined fields. (NENA)

Fast Re-route (FRR): An MPLS resiliency technology to provide fast traffic recovery upon link or router failures for mission critical services.

Federal Communications Commission (FCC): The FCC is an independent agency of the U.S. government that regulates interstate and international communications by radio, television, wire, satellite and cable.

Full-time Equivalent: Figure giving abstract employee number; a figure calculated from the number of full-time and part-time employees in an organization that represents these workers as a comparable number of full-time employees.

Geographic Information System (GIS): A computer software system that enables one to visualize geographic aspects of a body of data. It contains the ability to translate implicit geographic data (such as a street address) into an explicit map location. It has the ability to query and analyze data in order to receive the results in the form of a map. It can also be used to geographically display coordinates on a map i.e. Latitude/Longitude from a wireless 9-1-1 call. (NENA)

Gigabits per Second (Gbps): A unit of information transfer rate equal to one billion bits per second**.**

Graphical User Interface (GUI): A type of user interface that allows users to interact with electronic devices using images rather than text commands.

Heating, Ventilation and Air Conditioning (HVAC): HVAC refers to the technology of indoor environmental air temperature, humidity, and air quality control.

High-level Data Link Control (HDLC): A group of protocols or rules for transmitting data between network points (sometimes called nodes). Data is organized into a unit or frame and sent across a network to a destination that verifies its successful arrival. The HDLC protocol also manages the flow or pacing at which data is sent. HDLC is one of the most commonly-used protocols in Open Systems Interconnection (OSI) layer 2.

Hosted PSAP: A PSAP utilizing an ANI/ALI controller or a SIP Call Controller that serves multiple PSAPs/call groups.

Hot Standby Router Protocol (HSRP): A networking protocol that supports the non-disruptive failover of IP traffic in special circumstances. HSRP allows network hosts to look like they are using a single router and keep connected if the first hop router being used fails to respond. HSRP guards against the failure of the first hop router in a network infrastructure when the router's IP address cannot be found dynamically. HSRP normally joins several routers together to create a single virtual gateway that client machines and networks use. HSRP helps to ensure that only one of the virtual gateway's routers is working at any given time.

HTTP Enabled Location Determination (HELD): An IETF protocol for the retrieval of location information utilizing the HTTP protocol. (RFC 5985)

Hypertext Transport Protocol (HTTP): Hypertext Transport protocol typically used between a web client and a web server that transports HTML and/or XML. Often used as a transport for SOAP. (NENA)

Incumbent Local Exchange Carrier (ILEC): A telephone company that had the initial telephone company franchise in an area. (NENA)

Industry Collaboration Events (ICE): A NENA testing program that brings together vendors in an open, supportive, and collaborative environment that fosters a spirit of technical cooperation.

Initial Address Message (IAM): The first message sent in a SS7 ISUP call set-up by a switch or exchange to another partner exchange. IAM seizes/reserves a circuit between the exchanges for the call and contains the

information of numbers dialed by the calling party.

Integrated Services Digital Network (ISDN): International standard for a public communication network to handle circuit-switched digital voice, circuit-switched data, and packet-switched data. (NENA)

Integrated Services Digital Network User Part (ISUP): A message protocol to support call set up and release for interoffice voice call connections over SS7 Signaling. (NENA)

International Organization for Standardization (ISO): ISO is an international standard-setting body composed of representatives from various national standards organizations. The ISO promulgates worldwide proprietary, industrial, and commercial standards.

Internet Engineering Task Force (IETF): Lead standard setting authority for internet protocols. (NENA)

Internet Protocol (IP): The method by which data is sent from one computer to another on the Internet or other networks. (NENA)

Internet Protocol version 4 (IPv4): The fourth iteration of IP and the first version to be widely deployed.

Internet Protocol version 6 (IPv6): A version of IP that is intended to succeed IPv4, which is the communications protocol currently used to direct almost all Internet traffic. IPv6 will allow the Internet to support many more devices by greatly increasing the number of possible addresses.

Intrusion Detection System (IDS): A device or software application that monitors network or system activities for malicious activities or policy violations.

Intrusion Prevention System (IPS): Network security appliance that monitors network and/or system activities for malicious activity. An IPS identifies malicious activity, logs information about said activity, attempts to block/stop activity, and reports activity.

IP Multimedia Subsystems (IMS): A standardized architecture originally designed to provide telecom operators with metering (billing) and quality of service (bandwidth utilization) controls over IP and SIP-based voice, video, text, and other services that are transported on their cellular networks, both in the home service area and while roaming. IMS was originally conceived of as a means of extending Internet services to wireless networks while maintaining backward compatibility with the existing telecom business model, where the customer paid a bundled price for both access (the wireless network) and the services (voice minutes and text message counts). Today, the telecom industry sees IMS as a means of bringing about a convergence of wireless and wireline telecommunications services while using various access technologies.

Legacy Network Gateway (LNG): A media gateway solution with additional 9-1-1 specific features that allows legacy, TDM-based carrier networks to communicate with IP-based emergency services available in the ESInet.

Legacy PSAP Gateway (LPG): An NG9-1-1 Functional Element which provides an interface between an ESInet and an un-upgraded PSAP. (NENA)

Legacy PSAP: A PSAP that cannot process calls received via i3- defined call interfaces (IP-based calls) and still requires the use of CAMA or ISDN trunk technology for delivery of 911 emergency calls. (NENA)

Legacy technology: Includes wireline, wireless, and Voice over Internet Protocol (VoIP) devices connected through existing telephony switching and routing technologies to non-IP-enabled PSAPs.

Local Access and Transport Area (LATA): The geographical areas within which a local telephone company offers telecommunications services. (NENA)

Local Area Network (LAN): A transmission network encompassing a limited area, such as a single building or several buildings in close proximity. (NENA)

Local Exchange Carrier (LEC): A Telecommunications Carrier (TC) under the state/local Public Utilities Act that provide local exchange telecommunications services. Also known as Incumbent Local Exchange Carriers (ILECs), Alternate Local Exchange Carriers (ALECs), Competitive Local Exchange Carriers (CLECs), Competitive Access Providers (CAPs), Certified Local Exchange Carriers (CLECs), and Local Service Providers (LSPs). (NENA)

Location Information Server (LIS): 1) As described by the IETF, LIS is a device provided by a LAN operator, such as a business or institution, which devices that utilize the LAN may query to obtain their civil or geographic location. Examples are wireless access points that are programmed with the access point's location, and services that contain databases that associate Ethernet switch ports with Ethernet jack locations in buildings. The IETF specifies standard protocols used to identify and query a LIS, but leaves open how any particular LIS deployment determines location. 2) As often used by some vendors and NENA members, LIS is a legacy-like ALI database server that supports ALI queries using the LoST and HELD protocols. Such ALI (LIS) servers would be provided by 911 service providers.

Location Interwork Function (LIF): The functional component of a Legacy Network Gateway which is responsible for taking the appropriate information from the incoming signaling (i.e., calling number/ANI, ESRK, cell site/sector) and using it to acquire location information that can be used to route the emergency call and to provide location information to the PSAP. In a Legacy PSAP Gateway, this functional component takes the information from an ALI query and uses it to obtain location from a LIS. (NENA)

Location to Service Translation (LoST): A protocol that takes location information and a Service URN and returns a URI. Used generally for location-based routing. In NG9-1-1, used as the protocol for the ECRF and LVF. (NENA)

Location Validation Function (LVF): Validates that a given description of a location is both precise enough to route a 9-1-1 call and will be recognizable by dispatchers. In NENA i3 specifications, valid locations are routable locations, such as a latitude/longitude or postal address, not necessarily MSAG-validated.

Master Street Address Guide (MSAG): A data base of street names and house number ranges within their associated communities defining Emergency Service Zones (ESZs) and their associated Emergency Service Numbers (ESNs) to enable proper routing of 9-1-1 calls. (NENA)

Mean Opinion Score (MOS): A standardized measure of the quality of a telephone network from the human user's point-of-view. ITU document P.800 describes the conditions of the test where listeners sit in a quiet room, listen to standardized messages, and score voice quality as they perceive it on a scale from 1 to 5. Subsequent efforts have devised objective instrument-based measurements that track the subjective MOS scores very closely. For Voice over IP, these instrumental measurements are described in ITU P.862.

Mean Time Between Failures (MTBF): The predicted elapsed time between inherent failures that place a system out-of-service, of a system that is in operation. Assuming the system is instantly repaired, MTBF is an average obtained by dividing the total elapsed time by the number of failures occurring in that time interval. Planned or scheduled maintenance or downtime is not part of a MTBF calculation.

Megabits per Second (Mbps): A unit of information transfer rate equal to one million bits per second**.**

Message Transfer Part (MTP): Part of the Signaling System 7 (SS7) used for communications in public switched telephone networks (PSTNs). MTP is responsible for reliable, unduplicated and in-sequence transport of SS7 messages between communication partners.

Metropolitan Area Networks (MAN): A network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large LAN, but smaller than the area covered by a WAN. MAN is applied to the interconnection of networks in a city into a single larger network.

Management Information System (MIS): A MIS provides information that is needed to manage organizations efficiently and effectively. MIS is distinct from other information systems in that it is used to analyze operational activities in an organization.

Mobile Switching Center (MSC): The wireless equivalent of a Central Office, which provides switching functions for wireless calls. (NENA)

Monthly Recurring Charge (MRC): Charges that re-occur on a monthly basis.

Multi-Frequency (MF): A type of in-band signaling used on analog interoffice and 9-1-1 trunks. (NENA)

Multi-Protocol Label Switching (MPLS): A mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols.

Multi-purpose Internet Mail Extensions (MIME): An Internet standard that extends the format of email to support text in character sets other than ASCII, non-text attachments, message bodies with multiple parts, and header information in non-ASCII character sets. Use has grown beyond describing the content of email to describe content type in general. RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289 and RFC 2049 together define MIME specifications.

MyFloridaNet (MFN): An enterprise communications infrastructure dedicated for the exclusive use of State of Florida customers based on MPLS technology providing improved security and robust connectivity resulting in a highly available and highly reliable statewide communication network.

National Emergency Number Association (NENA): The National Emergency Number Association is a not-for-profit corporation established in 1982 to further the goal of "One Nation-One Number." NENA is a networking source and promotes research, planning and training. NENA strives to educate, set standards and provide certification programs, legislative representation and technical assistance for implementing and managing 9-1-1 systems. (NENA)

National Institute of Standards Technology (NIST): NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. (www.nist.gov)

NENA i3: The capability to receive IP-based SIP signaling and media for delivery of emergency calls and for originating calls conformant to the NENA 08-003 i3 standards. The key feature of NENA i3 is SIP location conveyance, whereby location information is transmitted with the SIP call setup messages via URI references or via MIME attached PDIF-LO values.

Network Address Translation (NAT): In computer networking, the process of network address translation (NAT, also known as network masquerading or IP-masquerading) involves re-writing the source and/or destination addresses of IP packets as they pass through a router or firewall. Most systems using NAT do so in order to enable multiple hosts on a private network to access the Internet using a single public IP address. (NENA)

Network Operations Center (NOC): A place from which administrators supervise, monitor and maintain a telecommunications network. A NOC is the focal point for network troubleshooting, software distribution and updating, router and domain name management, performance monitoring, and coordination with affiliated networks.

Network Management System (NMS): A combination of hardware and software used to monitor and administer a computer network.

Network Time Protocol (NTP): An IETF protocol for the distribution of time signals and the synchronization of clocks in large, diverse IP networks with widely varying data communication speeds. (RFC 1305)

Next Generation 911 (NG-911): NG9-1-1 is the next evolutionary step in the development of the 9-1-1 emergency communications system known as E9-1-1 since the 1970s. NG9-1-1 is a system comprised of managed IP-based networks and elements that augment present-day E9-1-1 features and functions and add new capabilities. NG9-1-1 will eventually replace the present E9-1-1 system. NG9-1-1 is designed to provide access to emergency services from all sources, and to provide multimedia data capabilities for PSAPs and other emergency service organizations. (NENA)

NG-911-specific Interwork Function (NIF): The functional component of a Legacy Network Gateway or Legacy PSAP Gateway which provides NG9-1-1-specific processing of the call not provided by an off-the-shelf protocol interwork gateway. (NENA) The key function of the NIF is to attach/detach location information to SIP messages in accordance with NENA i3 requirements.

North American Numbering Plan (NANP): Use of 10 digit dialing in the format of a 3 digit NPA followed by 3 digit NXX and 4 digit line number. NPA-NXX-XXXX. (NENA)

Numbering Plan Area (NPA): An established three-digit area code for a particular calling area where the first position is any number 2 through 9 and the last two (2) positions are 0 through 9. (NENA)

Numbering Plan Digit (NPD): A component of the traditional 8-digit 9-1-1 signaling protocol between the Enhanced 9-1-1 Control Office and the PSAP CPE. Identifies 1 of 4 possible area codes. (NENA)

Open Geospatial Consortium (OGC): An international industry consortium of nearly 500 companies, governmental agencies, and universities that participate in a consensus process to develop publicly available interface standards for the use and exchange of complex spatial information.

Open Shortest Path First (OSPF): An adaptive routing protocol for IP networks. OSPF uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system.

P-Asserted-Identity (PAI): Used among trusted SIP entities (typically intermediaries) to carry the identity of the user sending a SIP message as it was verified by authentication. See RFC 3325 section 9.1.

Points-of-Presence (POP): An artificial demarcation point or interface point between communications entities. An Internet POP is an access point to the Internet. It is a physical location that houses servers, routers, ATM switches and digital/analog call aggregators. It may be either part of the facilities of a telecommunications provider that the Internet service provider (ISP) rents or a location separate from the telecommunications provider.

Point-to-Point Protocol (PPP): A protocol that is used to establish a network link over a dedicated channel. It is widely used for Internet access. PPP is modular in design and can support different authentication protocols. (NENA)

Policy Routing Function (PRF): That functional component of an Emergency Services Routing Proxy that determines the next hop in the SIP signaling path using the policy of the nominal next element determined by querying the ECRF with the location of the caller. A database function that analyzes and applies ESInet or PSAP state elements to route calls, based on policy information associated with the next-hop. (NENA)

Premise (P): A building or structure that houses telecommunications equipment and/or demarcation points, such as an office, PSAP, or data center.

Premise Edge (PE): Generally a router between one network service provider's area and areas administered by other network providers or customers, often located at the customer or demarcation site.

Presence Information: In telecommunications and computer networks, presence information is information such as the location or status of a potential communications partner. For example, many instant messaging systems list which partners are on-line (available), which partners are away, and which partners are busy or do not wish to be disturbed. The busy lamps on some telephone systems that show other telephones that are currently in use is another example of presence information.

Presence Information Data Format (PIDF): The Presence Information Data Format is specified in IETF RFC 3683; it provides a common presence data format for presence protocols, and also defines a new media type. A presence protocol is a protocol for providing a presence service over the Internet or any IP network. (NENA)

Presence Information Data Format – Location Objects (PIDF-LO): Provides a flexible and versatile means to represent location information using an XML schema. In NENA i3, the PDIF-LO is transmitted by SIP messages as a MIME attachment.

Private Branch Exchange (PBX): A private telephone switch that is connected to the Public Switched Telephone Network. (NENA)

Protocol Interworking Function (PIF): That functional component of a Legacy Network Gateway or Legacy PSAP Gateway that interworks legacy PSTN signaling such as ISUP or CAMA with SIP signaling. (NENA)

Pseudo Automatic Number Identification (pANI): A telephone number used to support routing of wireless 9-1-1 calls. It may identify a wireless cell, cell sector or PSAP to which the call should be routed. Also known as a routing number. (NENA)

Public Safety Answering Point (PSAP): An entity operating under common management which receives 9-1-1 calls from a defined geographic area and processes those calls according to a specific operational policy. (NENA)

Public Security Control Zone (PSCZ): A security pass-through zone that connects to the public Internet on one side and the Core NG-911 Routing Service zone on the other side.

Public Switched Telephone Network (PSTN): The network of equipment, lines, and controls assembled to establish communication paths between calling and called parties in North America. (NENA)

Quality of Service (QoS): As related to data transmission a measurement of latency, packet loss and jitter. (NENA) As a feature of IP and underlying networks, mechanisms intended to provide certain applications (such a voice transmission) minimum levels of service sufficient to obtain a specified level of quality for those applications. For example, the QoS mechanism may give IP packets carrying voice signals transport priority over other IP packets.

Real-time Text Protocol (RTTP): Object-oriented bidirectional messaging protocol for delivering real-time text data over IP networks.

Real-time Transport Protocol (RTP): A network protocol used to carry packetized audio and/or video traffic over an IP network that helps ensure that packets get delivered in a timely way. (NENA)

Request for Assistance (RFA): An IP-based 911 solution that initially delivers voice-only emergency calls via IP-enabled selective routers, via SIP, and delivers ALI utilizing legacy ALI systems.

Request for Assistance Interface (RFAI): Interface between an emergency services next generation network and a PSAP, as defined by ATIS 0500019.2010, which supports the transition from legacy systems to IP-based networks.

Request For Assistance User Agent (RFAUA): A SIP UA that is a component within an RFA-type IP-based 911 solution.

Request for Comment (RFC): A formal document from the IETF that is the result of committee (working group) drafting and subsequent review through a formal process. Some RFCs are informational only. Other RFCs become standards. If an RFC becomes a standard then, except for errata, no further comments or changes are permitted. However subsequent RFCs may supersede or elaborate on all or parts of previous RFCs.

Request for Proposal (RFP): An invitation is presented to vendors to submit a proposal on a specific commodity or service. The RFP process allows the risks and benefits to be identified clearly up front.

Secure Shell (SSH): A network protocol for secure data communication, remote shell services or command

execution and other secure network services between two networked computers that it connects via a secure channel over an insecure network.

Security Information Management (SIM): In computer security, refers to the collection of data, such as log files, into a central repository for trend analysis.

Sensitive data: Data or information that the PSAP has indentified to be kept from disclosure.

Service Level Agreement (SLA): A contract between a service provider and the end user, which stipulates and commits the service provider to a required level of service. (NENA)

Service Provider: An entity providing one or more of the following 9-1-1 elements: network, CPE, or data base service. (NENA)

Session Border Controller (SBC): A commonly available functional element that provides security, NAT traversal, protocol repair and other functions to VoIP signaling such as SIP. A component of a Border Control Function. (NENA)

Session Description Protocol (SDP): An IETF format (RFC 4566) for describing streaming media (such as voice, video, or text) initialization parameters for the purposes of session announcement, session invitation, and parameter negotiation. SDP does not deliver media itself, but is used for negotiation between end points of media type, format, and all associated properties.

Session Initiation Protocol (SIP): An IETF defined protocol (RFC3261) that defines a method for establishing multimedia sessions over the Internet. Used as the call signaling protocol in VoIP, i2 and i3. (NENA)

Signaling System 7 (SS7): An out-of-band signaling system used to provide basic routing information, call set-up and other call termination functions. Signaling is removed from the voice channel itself and put on a separate data network. (NENA)

Simple Network Management Protocol (SNMP): A protocol defined by the IETF used for managing devices on an IP network. (NENA)

Spatial Information Function (SIF): A term encompassing geospatial-related information that may be stored in a GIS database and may be accessible via the LoST protocol, including information beyond what is immediately required to route an emergency call to the appropriate destination. Examples of such information include the geographic service areas of utility companies (electric, gas, telecommunications), railroad control towers, heavy equipment operators, emergency shelter locations, large building floor plans, locations of Automatic Emergency Defibrillators, and specialized hiking and water rescue teams.

Stand-alone PSAP: PSAP utilizing equipment and services (e.g., an ANI/ALI controller) that are located on-site and serve only one PSAP.

Standards Development Organization (SDO): An entity whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise maintaining standards that address the interests of a wide base of users outside the standards development organization. (NENA)

Sub-state: Any IP-capable 911 system or ESInet, distinct from the statewide NG-911 Routing Service, located

within the state of Florida and which performs emergency call routing functions. These sub-state systems are typically operated by a local authority or regional consortium.

Synchronous Optical Network (SONET): High speed digital transport over fiber optic networks using synchronous protocol. (NENA)

Telecommunications Device for the Deaf (TDD): A device capable of information interchange between compatible units using a dial up or private-line telephone network connections as the transmission medium. ASCII or Baudot codes are used by these units. (per EIA PN-1663) (NENA)

Telecommunications Industry Alliance (TIA): A lobbying and trade association, the result of the merger of the USTA (United States Telephone Association) and the EIA (Electronic Industries Association). (NENA)

Telecommunications Service Priority (TSP): A procedure used by a telephone company to establish priorities in deciding which lines and trunks to restore subsequent to an outage. Generally, the highest priority goes to federal law enforcement and military usage, with local emergency services (including 9-1-1) and medical facilities following. Established by the National Communications System Office. (NENA)

Teletypewriter (TTY): A device capable of information interchange between compatible units using a dial up or private-line telephone network connections as the transmission medium. ASCII or Baudot codes are used by these units. (per EIA PN-1663) (NENA)

Traffic Engineering (TE): A method of optimizing the performance of a telecommunications network by dynamically analyzing, predicting and regulating the behavior of data transmitted over that network.

Transmission Control Protocol (TCP): The end to end reliability protocol that recognizes and corrects lower layer errors caused by connectionless networks. (NENA)

Transport Layer Security (TLS): A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third-party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

A protocol that provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. (IETF)

Uniform Resource Identifier (URI): A predictable formatting of text used to identify a resource on a network (usually the Internet). (NENA)

Uniform Resource Locator (URL): A URL is a URI specifically used for describing and navigating to a resource (e.g. http://www.nena.org). (NENA)

Uniform Resource Name (URN): An Internet location-independent resource identifier or name, that unlike URL, has persistent significance - that is, the owner of the URN can expect that a person or program will always be able to find the resource. URN is a type of URI.

Uninterruptible Power Supply (UPS): A backup system designed to provide continuous power in the event of a

commercial power failure or fluctuation. (NENA)

User Agent (UA): As defined for SIP in IETF RFC 3261, the User Agent represents an endpoint in the IP domain, a logical entity that that can act as both a user agent client (UAC) that sends requests, and as user agent server (UAS) responding to requests. (NENA)

User Datagram Protocol (UDP): One of several core protocols commonly used on the Internet. Used by programs on networked computers to send short messages, called datagrams, between one another. UDP is a lightweight message protocol, compared to TCP, is stateless and more efficient at handling lots of short messages from many clients compared to other protocols like TCP. Because UDP is widely used, and also since it has no guaranteed delivery mechanism built in, it is also referred to as Universal Datagram Protocol, and as Unreliable Datagram Protocol. (NENA)

Virtual Private Network (VPN): A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. (NENA)

Virtual Routing and Forwarding (VRF): A technology included in IP network routers that allows multiple instances of a routing table to exist in a router and work simultaneously. This increases functionality by allowing network paths to be segmented without using multiple devices. Because traffic is automatically segregated, VRF also increases network security and can eliminate the need for encryption and authentication.

Voice over Internet Protocol (VoIP): Provides distinct packetized voice information in digital format using the Internet Protocol. The IP address assigned to the user's telephone number may be static or dynamic. (NENA)

Wide Area Network (WAN): Network using common carrier-provided lines that covers an extended geographic area. (NENA)

Wireless ALI Service Provider (WASP): A service provider that interfaces wireless carrier mobile positioning centers with legacy 9-1-1 service providers. Typically, the WASP provides a pANI/Emergency Services Routing Key (ESRK) for each wireless 9-1-1 call based on the cellular tower used by the caller, and posts the location information into an ALI server under the ESRK. The wireless 9-1-1 call then appears much like a wireline 9-1-1 call to the legacy selective router, legacy PSAP, and legacy ALI system.

4.0.2 Intent

The following technical specifications describe the statewide Next Generation 911 (NG-911) Routing Service that the State of Florida desires to implement in the near future. This system is based on Internet Engineering Task Force (IETF) Session Initiation Protocol (SIP) with location conveyance, on National Emergency Number Association (NENA) i3 design elements, and on the needs of Florida.

The successful Respondent will provide a robust and reliable NG-911 Routing Service that will deliver 911 calls from various Emergency Call Origination Networks (ECONs) to subscribing counties, public safety answering points (PSAPs), and sub-state NG-911 systems. The goal is to provide a robust reliable NG-911 Routing Service for the benefit of the residents and visitors to the state.

The overall system will be operated in coordination with SUNCOM, which will supply highly available wide-area Internet Protocol (IP) network connectivity and related services. Respondents will benefit from a careful study of the on-line resources available for the MyFloridaNet system, as well as the information contained within this document. Respondents should examine the MyFloridaNet system user guide for an understanding of the service nature and collaborative system that is envisioned by the Florida Department of Management Services (Department or DMS).

The Department is aware of several solutions that may meet some requirements in this document. While a single Respondent will be selected as the prime contractor, Respondents are encouraged to work collaboratively with the service providers to provide a coordinated response meeting the specifications requirements.

4.0.3 Specifications Organization

Specifications are organized for ease of describing the functions required for the Florida NG-911 Routing Service; this organization should be followed when responding to this process. However, the organization of the specifications in this document should NOT be considered as a prescription for the organization of the components of a proposed solution. Respondents should develop and propose the design for the solution that is in compliance with the specifications. The proposed solution shall operate as a single statewide system.

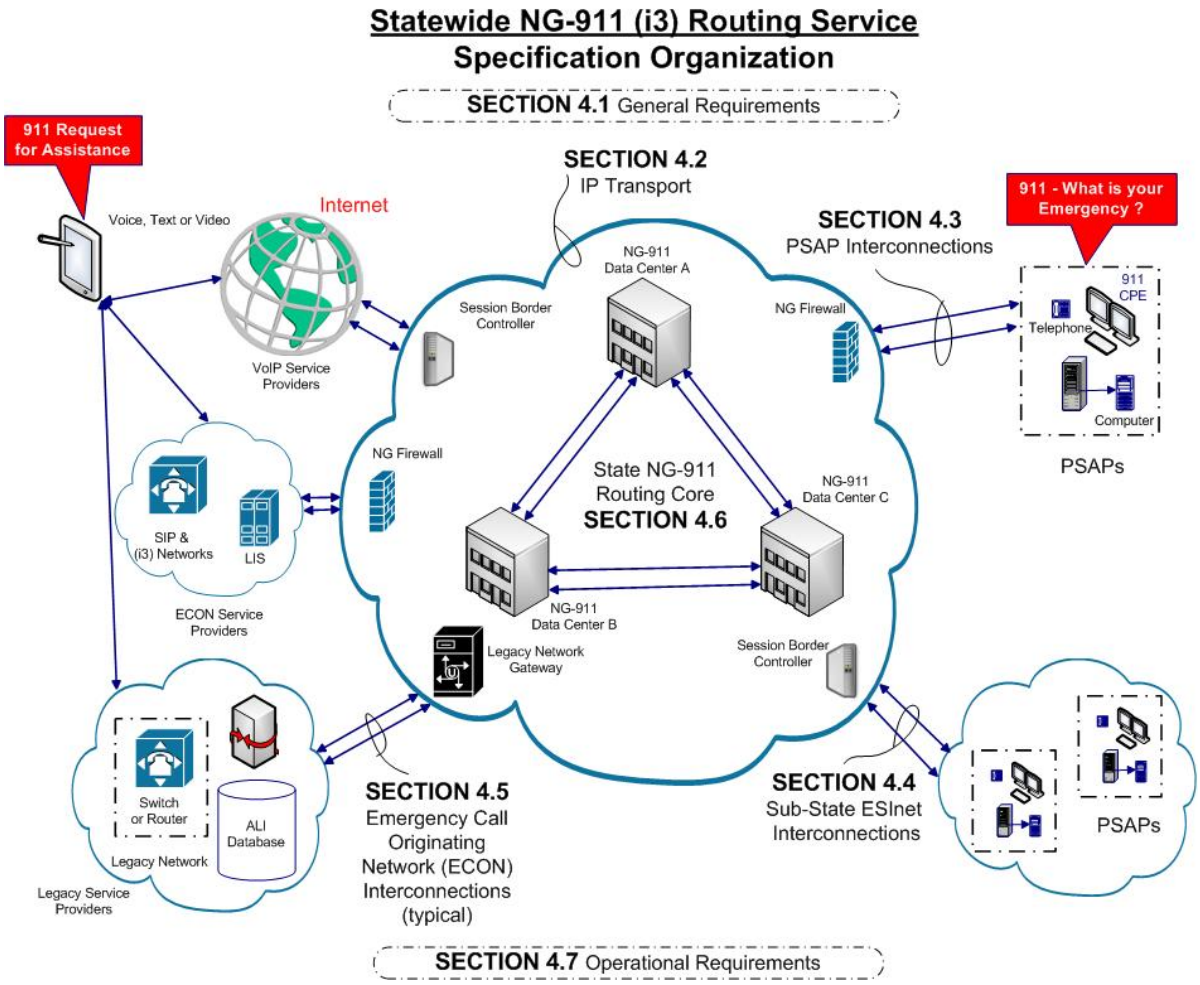


Figure 1—NG-911 Routing Service

Section 4.1: General Requirements
This section establishes the general requirements of the NG-911 Routing Service and describes the level of detail expected in the response.

Section 4.2: IP Transport Requirements
This section describes requirements of the IP transport component for the NG-911 Routing Service utilizing MyFloridaNet as transport.

Section 4.3: Individual PSAP and Hosted CPE Interconnection Requirements
This section describes the types of interfaces and system interface requirements for PSAP integration into the Florida NG-911 Routing Service.

Section 4.4: Sub-state ESInet Interconnection Requirements
This section describes the types of interfaces to sub-state Emergency Services IP network (ESInet) locations and the system interface requirements to interconnect these sub-state ESInets into the statewide Florida NG-911 Routing Service.

Section 4.5: Call Origination Provider Interconnection Requirements
This section describes the types of interfaces from call origination networks and the system interface requirements to interconnect the call origination networks into the statewide Florida NG-911 Routing Service.

Section 4.6: Core NG-911 Function Requirements
This section describes the application level functions and specific functions that are required to occur in the core NG-911 Routing Service. The detailed functional requirements for each application describe the desired function of the applications.

Section 4.7: Operational Requirements
This section describes the operational functions that will be required from the successful Respondent.

4.0.4 Current Environment

4.0.4.1 Existing Sub-state ESInets

There are two countywide (Brevard and Palm) and four regional systems in current deployment or implementation. Existing sub-state data may change. Respondents should verify that the information below is current.

- Lake/Orange Regional Project – Still in implementation, CenturyLink and AT&T
  - Lake County – 8 PSAPs all with MyFloridaNet circuits connected and CenturyLink selective router
  - Orange County – 10 PSAPs all with MyFloridaNet circuits connected; eight connections; two PSAPs are co-located

- Okaloosa/Walton Regional Project – Still in implementation, CenturyLink
  - Okaloosa County – 9 PSAPs all with MyFloridaNet circuits connected

  - Walton County – 3 PSAPs, currently one primary with MyFloridaNet circuits connected; secondary PSAPs being connected

- St. Lucie/Martin Regional Project – Installation complete and operational using Intrado's "Intellegent Emergency Network" (IEN) product
  - Martin County – 4 PSAPs all with IEN circuits connected
  - St. Lucie County – 1 PSAP and 1 backup PSAP connected with IEN circuit
  - Charlotte County – 2 primary PSAPs and 1 backup PSAP connected with a county network and IEN connectivity
  - Levy County – 1 PSAP connected with IEN Circuit

- North Florida Routing System (NFRS) Project – Still in development (limited to call transfer and backup)
  - Baker County – 1 primary PSAP and 1 backup PSAP connected with MyFloridaNet circuits (ECS-1000 & Solacom routers)
  - Bradford County – 1 primary PSAP connected with MyFloridaNet circuit (Solacom router)
  - Clay County – 3 primary and 1 secondary PSAPs; two connections with MyFloridaNet circuits (two Solacom routers)
  - Duval County – 5 primary and 2 secondary PSAPs and 1 backup PSAP; systems in process of upgrade and replacement
  - Dixie County – 1 primary PSAP connected with MyFloridaNet circuit (Solacom router)
  - Lafayette County – 1 primary PSAP connected with MyFloridaNet circuit (ECS-1000 router)
  - Leon County – 2 primary and 5 secondary PSAPs; two connections with MyFloridaNet circuits (two Solacom routers)
  - Liberty County – 1 primary PSAP connected with MyFloridaNet circuit (ECS-1000 router)
  - Madison County – 1 primary PSAP connected with MyFloridaNet circuit (Solacom router)
  - Putnam County – 1 primary PSAP and 1 backup PSAP connected with MyFloridaNet circuit (two Solacom routers)
  - St. Johns County – 2 primary PSAPs and 1 backup PSAPs; one connection with MyFloridaNet circuit (one Solacom router)
  - Suwannee County – 1 primary PSAP connected with MyFloridaNet circuit (ECS-1000 router) (replacement system in procurement)
  - Taylor County – 1 primary PSAP connected with MyFloridaNet circuit (ECS-1000 router) (replacement system in procurement)

Table 1—PSAP and Call Data by County and Carrier

County	Number of Primary PSAPs	Number of Secondary PSAPs	Number of Backup PSAPs	Number of 911 Calls per Year	County Population	Sub-state System
Brevard	10	1	0	341,191	545,184	AT&T
Palm Beach	18	1	2	803,687	1,325,758	AT&T
AT&T Total	28	2	2	1,144,878	1,870,942	
Lake	7	1	0	206,495	298,265	CenturyLink
Orange	7	3	0	1,099,578	1,157,342	AT&T

County	Number of Primary PSAPs	Number of Secondary PSAPs	Number of Backup PSAPs	Number of 911 Calls per Year	County Population	Sub-state System
Total	14	4	0	1,306,073	1,455,607	
Okaloosa	3	6	1	117,530	181,679	CenturyLink
Walton	1	2	0	32,904	55,450	CenturyLink
CenturyLink Total	4	8	1	150,434	237,129	
Charlotte	2	0	1	73,694	160,463	Intrado IEN
Levy	1	0	1	24,153	40,767	Intrado IEN
Martin	2	1	1	116,132	146,689	Intrado IEN
St. Lucie	1	0	1	332,181	279,696	Intrado IEN
IEN Total	6	1	4	546,160	627,615	
Baker	1	0	1	15,415	26,927	NFRS
Bradford	1	0	1	17,390	28,662	NFRS
Clay	3	1	0	91,428	191,143	NFRS
Dixie	1	0	1	6,945	16,385	NFRS
Duval	5	2	1	780,507	864,601	NFRS
Lafayette	1	0	0	5,786	8,752	NFRS
Leon	2	5	1	183,175	276,278	NFRS
Liberty	1	1	1	4,451	8,370	NFRS
Madison	1	0	0	15,286	19,298	NFRS
Putnam	1	0	1	59,375	74,052	NFRS
St. Johns	2	0	1	78,566	192,852	NFRS
Suwannee	1	0	0	26,950	43,215	NFRS
Taylor	1	0	1	14,202	22,500	NFRS
NFRS Total	21	9	9	1,299,476	1,773,035	

4.0.4.2 MyFloridaNet

This description is intended to provide a prospective Respondent with a high-level overview of the MyFloridaNet network. The MyFloridaNet system shall be used by the NG-911 Routing Service to provide wide-area IP transport.

The current MyFloridaNet system will be nearing the end of its current contract and will go through a procurement process to update and improve the network during the anticipated period of operation of the NG-911 Routing Service.

The Department is the state entity that operates the State's telecommunications service provider. The Department's portfolio includes the Public Safety Bureau, which encompasses the State's Enhanced 911 (E911)

program, which provides support to the E911 Board and MyFloridaNet, which provides telecommunication services for state and local governments and non-profits operating in Florida.

MyFloridaNet is the result of the consolidation of five separate state IP networks into one network, which was completed in March 2008. The Department requires that MyFloridaNet be utilized as the wide-area IP transport for the NG-911 Routing Service.

Prospective Respondents should consult the www.dms.myflorida.com website for authoritative details concerning the DMS organizational structure. This site contains references to legislation that govern the scope and operation of the various departments and agencies.

This website is also the first source of information concerning the features, capabilities, and characteristics of MyFloridaNet. The starting web page for MyFloridaNet technical details may be found at:

http://www.dms.myflorida.com/suncom/suncom_products_and_pricing/data_transport_services/myfloridanet/mfn_resources.

The Department does not own actual telecommunications infrastructure, but procures dedicated communications infrastructure and infrastructure services under contract with Service Level Agreements (SLAs) from commercial telecommunications providers that operate in Florida. In the same way, the NG-911 Routing Service provider will provide NG-911 resources and services to MyFloridaNet, under contract with SLAs, in order to provide the State with a state-level NG-911 Routing Service.

4.0.4.2.1 Description of MyFloridaNet Core

The MyFloridaNet Core consists of a meshed fiber structure comprised of multiple overlapping rings. The diagram on the following page (Figure 2) presents an overall depiction of MyFloridaNet Core topology. The current version of this diagram is available at:

http://www.dms.myflorida.com/suncom/suncom_products_and_pricing/data_transport_services/myfloridanet/mfn_resources/engineering_diagrams

Additional diagrams of interest to the NG-911 Routing Service provider may also be found at this link.

The MyFloridaNet Core Points-of-Presence (POPs) are located in telephone company central offices in ten major Florida cities as depicted in the diagram below. Hereafter, these POPs are referred to as IP Core Nodes. (Some MyFloridaNet literature may refer to these sites as IP nodes.)

The remainder of this page is left blank.

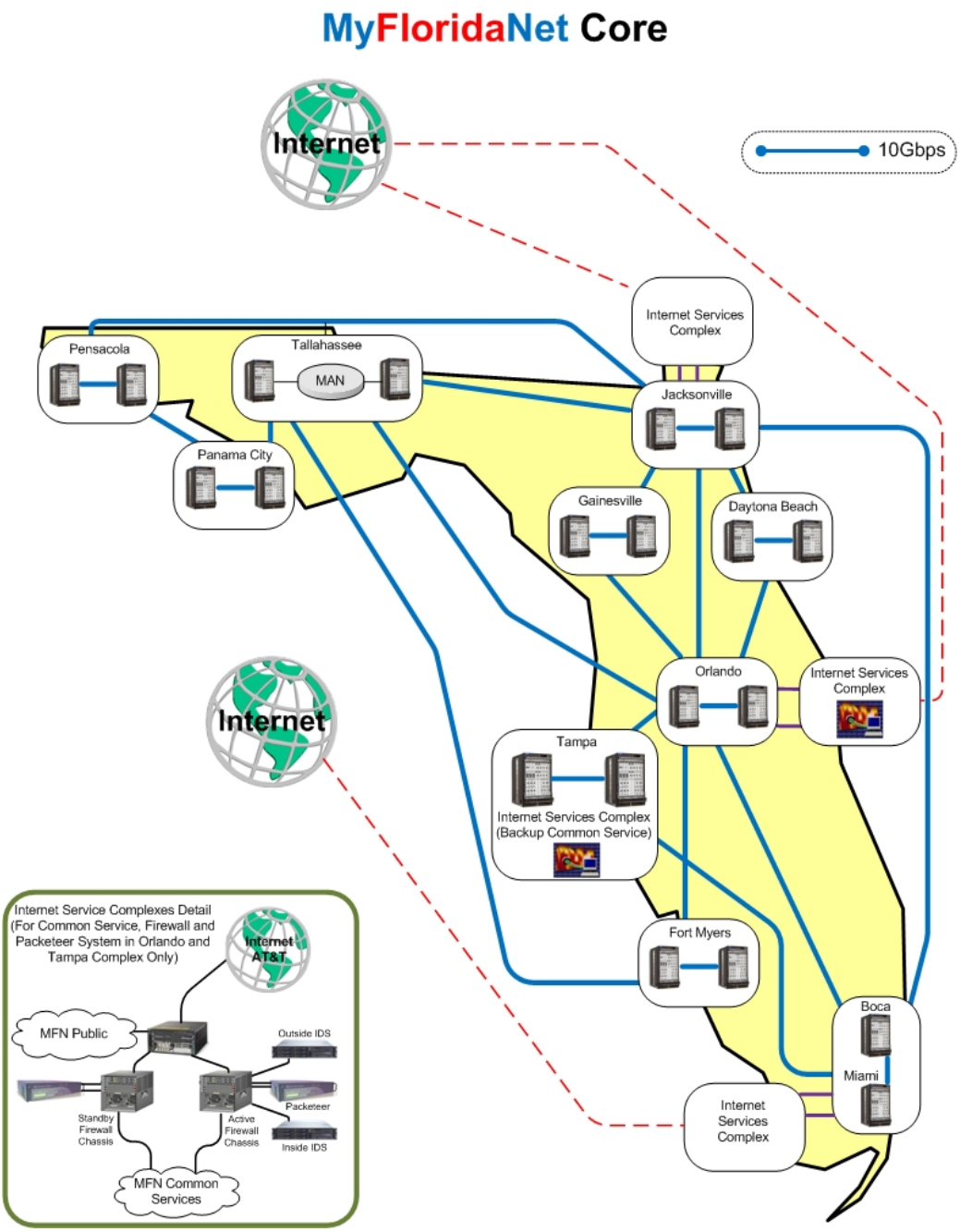


Figure 2—MyFloridaNet Core

The facilities housing the MyFloridaNet IP Core Nodes are built to common telephone company central office standards, and can be assumed to essentially meet or exceed Telecommunications Industry Alliance (TIA) Tier 3 requirements including diverse cable entrances; physical security; fire suppression; uninterruptible power supply (UPS) and generator-backed power; adequate heating, ventilation and air conditioning (HVAC) systems; and a high-level of documentation and record-keeping.

The blue links in the MyFloridaNet Core network diagram represent dedicated (to MyFloridaNet) ten gigabits per second (Gbps) data connections between the IP Core Nodes. The telephone contractor(s) that supply these links provision the MyFloridaNet links utilizing various methodologies (e.g., Dense Wavelength Division Multiplexing [DWDN]). Regardless of the provisioning, MyFloridaNet is guaranteed a 10 Gbps timeslot by contract.

Each IP Core Node houses two carrier-grade Juniper M320 routers dedicated to MyFloridaNet and fully visible to MyFloridaNet engineers. That is, MyFloridaNet can view the configuration of these routers directly, and can make configuration change requests to the MyFloridaNet service provider. Interestingly, MyFloridaNet provides MyFloridaNet customers safe read-only access to these router configurations (via a proxy server) so that MyFloridaNet users can see for themselves how MyFloridaNet is configured with respect to the services transported by MyFloridaNet. This capability provides the NG-911 contractor the opportunity to verify and monitor the operation of the ESInet circuits related to the NG-911 Routing Service nearly as if they owned it themselves.

The MyFloridaNet IP Core infrastructure is designed to provide five nines (99.999 percent) availability throughout.

As the following diagram (Figure 3) of Florida local access transport areas (LATAs) depicts, MyFloridaNet IP Core Nodes are located within each LATA in the state.

MyFloridaNet also provides access to a number of commercial metropolitan area networks (MANs) where they exist. By contract, the technical requirements and SLAs for layer 2 and layer 3 MyFloridaNet services provisioned via these MANs mirror those of the MyFloridaNet Core network itself. MyFloridaNet services provisioned via the MANs follow the same Quality of Service (QoS) and Class of Service (CoS) treatments as the MyFloridaNet Core. Connection speeds in various increments from 1.5 megabits per second (Mbps) up to 10 Gbps are available in selected areas via the MANs.

The remainder of this page is left blank.

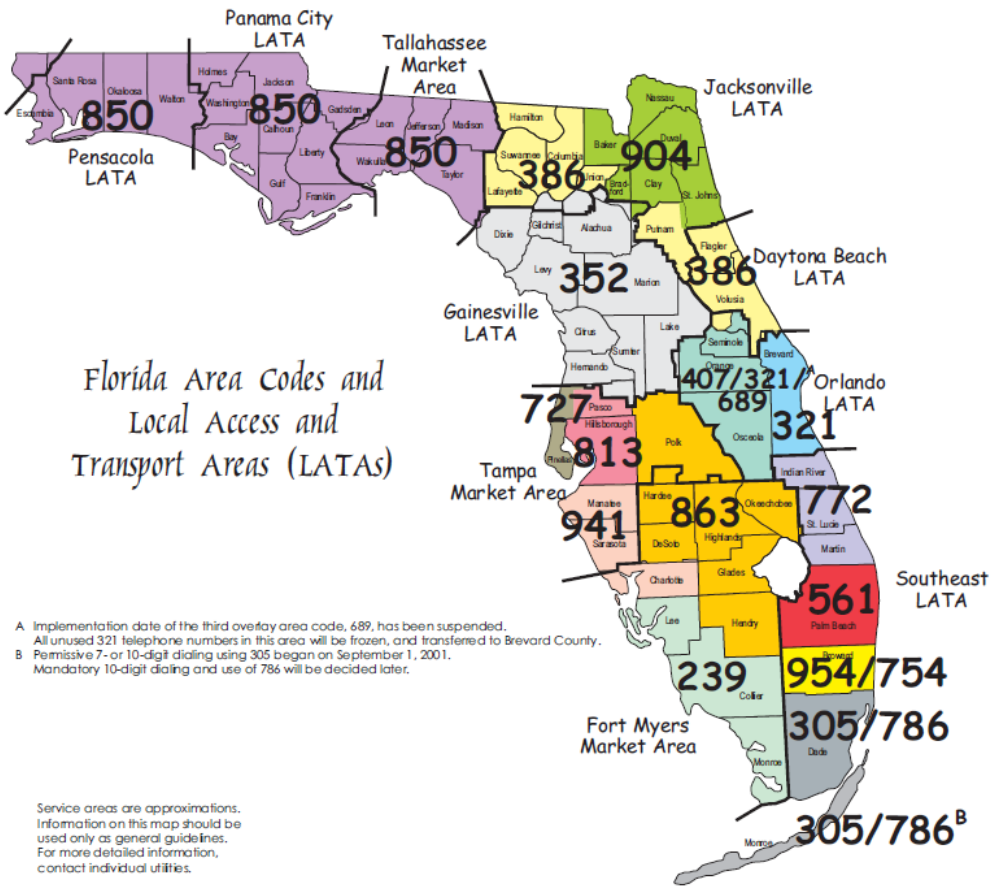


Figure 3—Florida LATAs

Interconnection with the MyFloridaNet Core or MyFloridaNet MANs is via layer 2 Ethernet.

MyFloridaNet has a variety of access network arrangements, including Digital Signal, level 1 (DS1); Frame Relay, Digital Subscriber Line (DSL); Metro Ethernet; mobile cellular; and satellite. Primary ESInet access connections should be restricted to DS1, Frame Relay, or Metro Ethernet facilities; mobile cellular or satellite may be considered for backup ESInet access connections. The following diagram (Figure 4) depicts MyFloridaNet access arrangements. SLAs for MyFloridaNet services are also available at the links listed previously.

The remainder of this page is left blank.

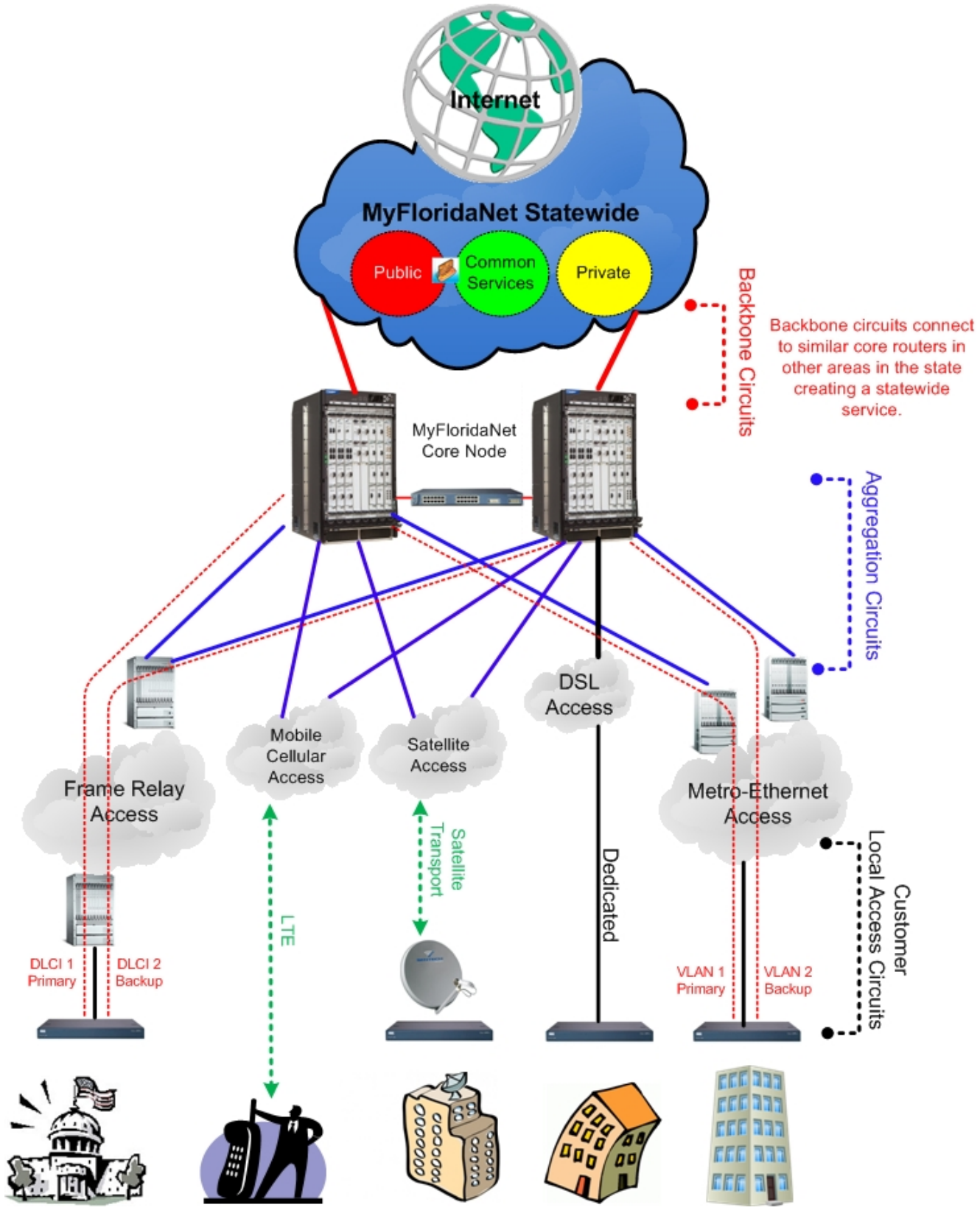


Figure 4—MyFloridaNet Access

Return to Index

4.0.4.2.2 MyFloridaNet Virtual Networks

As mentioned previously, MyFloridaNet represents the consolidation of several statewide IP infrastructures.

MyFloridaNet uses multi-protocol label switching (MPLS) and virtual route forwarding (VRF) technologies to partition MyFloridaNet resources into separate layer 2 and separate layer 3 network infrastructures. These partitions provide each MyFloridaNet customer or major application with their own slice of MyFloridaNet bandwidth and with their own private layer 2 and/or layer 3 network infrastructures.

Within VRF, MyFloridaNet customers may, subject to the MyFloridaNet naming conventions, addressing, or IPv6 master plan, establish and implement their own local area IP addressing scheme, their own security/access policies, and their own network monitoring practices. Interconnection of VRF with other IP networks occurs only via IP routing and firewall functions, which may be provided by the MyFloridaNet Core routers or via other arrangements.

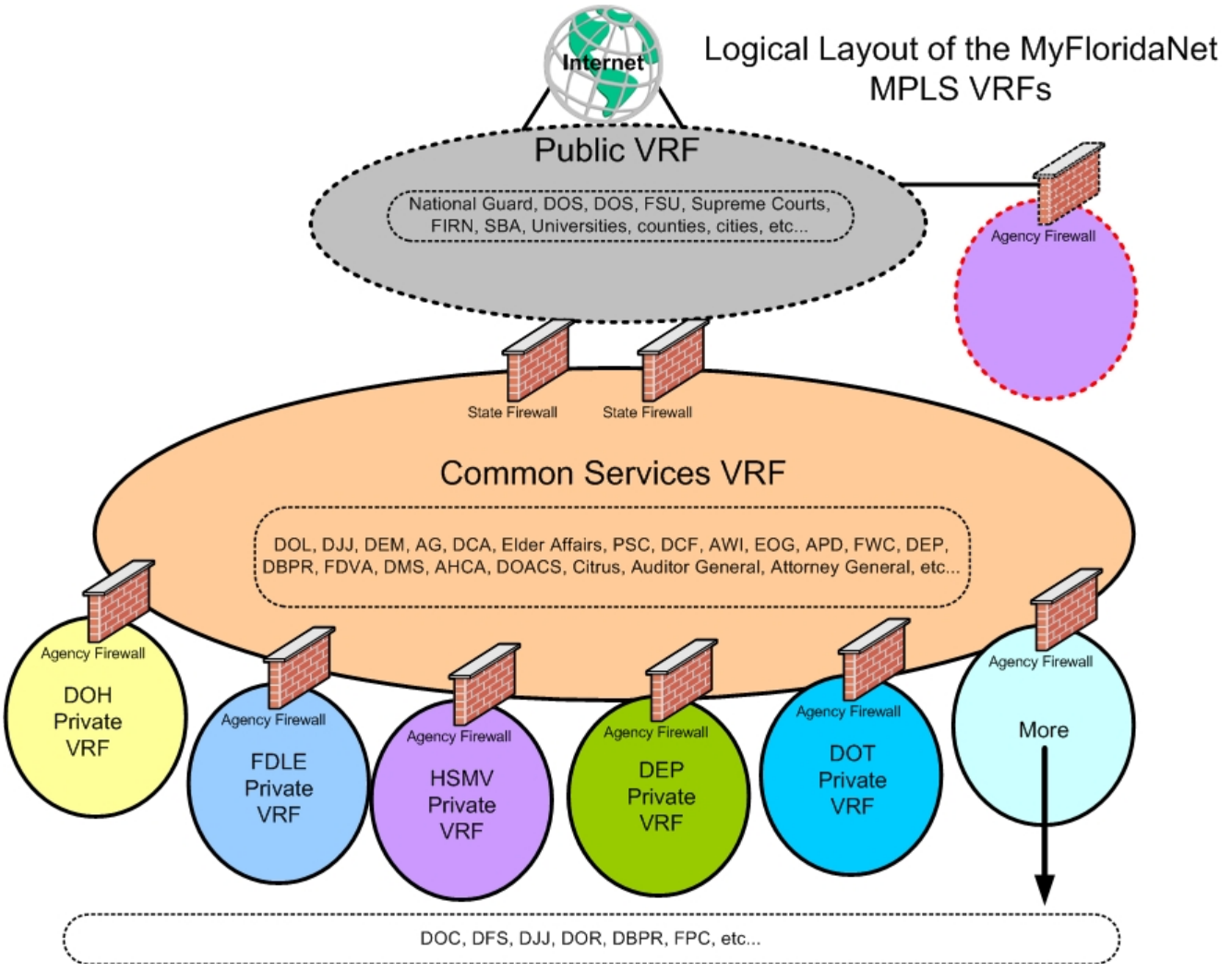


Figure 5—MPLS VRFs

Return to Index

A private, dedicated VRF will be provided for the ESInet. The following diagram (Figure 6) depicts the 911 VRF in the context of the other MyFloridaNet partitions and applications.

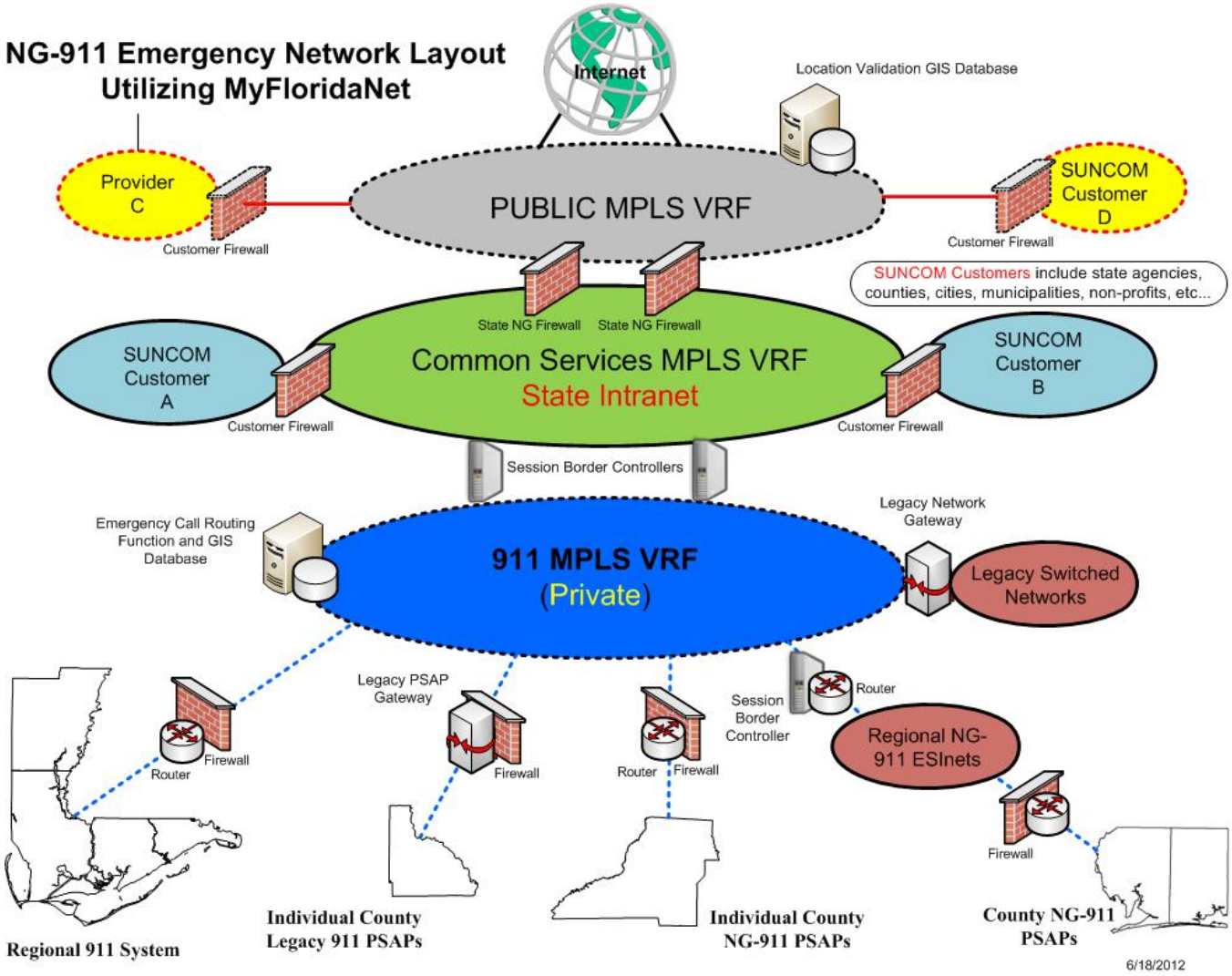


Figure 6—NG-911 Emergency Network Layout

The NG-911 Routing Service provider, together with Florida public safety officials, will specify the terms and conditions of interconnections between the NG-911 Routing Service dedicated IP space and other IP networks, including sub-state ESInets operated by local authorities, and carrier and PSAP IP networks. Such interconnections must also comply with the specifications herein.

The QoS scheme for the ESInet VRF shall be differentiated services (DiffServ) in compliance with the MyFloridaNet design requirements summarized below.

The Florida NG-911 Routing Service shall operate in the MyFloridaNet 911 VRF. The specifications within this document create additional requirements for the Florida NG-911 Routing Service. For example, the Florida NG-911 Routing Service is required to be exclusively an IPv6 infrastructure.

- 99.999 percent availability and uptime for core/backbone resources.
  - Virtual private network (VPN) naming convention in compliance with Request for Comment (RFC) 2685.
- Premise (P) and Premise Edge (PE) router console access must utilize Secure Shell (SSH) only.
- P and PE routers must not have interfaces directly exposed to the Internet.
- The Core supports Open Shortest Path First (OSPF) v3 and Border Gateway Protocol (BGP)-4 routing protocols, with extensions for IPv6.
- The Core implements a single MPLS domain (avoiding Inter-AS VPNs).
- The Core supports several techniques for multi-path load balancing, which improves service offering capabilities.
- The Core supports customer native IPv6 during the initial implementation. The State will run dual protocol stacks until IPv4 can be eliminated. (Note: Dual protocol stacks do not apply to the Core NG-911 Routing Service.) The NG-911 Routing Service provider and customers shall strictly adhere to the IPv6 addressing plan for both the Core backbone and customer networks. Core routing equipment is used to enforce the addressing plan's policies and rules.
- The Core supports MPLS DiffServ (Experimental bit), MPLS Traffic Engineering (TE) and future service options, such as MPLS DiffServ-aware TE (DS-TE).
- Fast Re-route (FRR) is supported for all implementations.
- The Core supports QoS for all access types (Frame Relay, Ethernet, and Point-to-point Protocol [PPP]/ high-level data link control [HDLC], etc.) over MPLS.
- The Core is designed and prepared to support future inter-provider QoS.
- The Core supports the current MyFloridaNet QoS classes listed in Table 2.

Table 2—MyFloridaNet QoS Classes

Class	Description	DSCP Marking	DSCP (Decimal Value)
Voice	Voice over IP (VoIP)	EF	46
Video	Interactive Video	AF41	34
Application	Priority Data	AF21	18
Best Effort	All other Traffic	BE	0
Signaling	Call setup & control	AF31	26
Emergency Public Safety Real-time	Priority VoIP	AF43	38

4.0.4.2.3 MyFloridaNet Services

Prospective Respondents are advised to consult the MyFloridaNet website for a complete list and description of MyFloridaNet services. A very high-level overview of these services follows:

- Domain Name Services – designed to meet the high-availability requirements of MyFloridaNet; both public Internet and private (hidden) Domain Name Servers (DNS) are provided
- Network Time Protocol (NTP) Stratum I servers
- IP multicast
- Contracted 24/7 network monitoring service
- MyFloridaNet Network Operations Center (NOC)
- Web-accessible traffic monitoring (down to 5-minute intervals) and operational reports
- Indirect read-only access (via proxy servers) to routers and devices applicable to the VRF service domain and operations, such as customer-specific access control lists (ACLs) and Simple Network Management Protocol (SNMP) status of VRF interfaces in MyFloridaNet routers and devices
- E-mail and pager alerts based on bandwidth, latency, jitter, error rates, and other thresholds
- Customer access to a rich and powerful set of operational, performance, and diagnostic tools via a single login

MyFloridaNet engineers continuously monitor the health and status of MyFloridaNet using powerful monitoring tools. As a general rule, these same tools are available via web browsers for the use of MyFloridaNet customers and users. A complete description of the tools can be found at www.dms.myflorida.com.

4.0.4.2.4 MyFloridaNet Monitoring and Security

MyFloridaNet incorporates tools, processes and procedures to provide highly reliable network and services. PSAPs and their respective vendors shall make themselves familiar with those tools, processes and procedures and shall provide documentation that supports that understanding. Graphical representation of interworking shall be used where appropriate.

At a high-level, the general tools currently include the following:

- Single sign-on to MyFloridaNet portal to access all tools except QRadar (Security tool). (Figure 7)

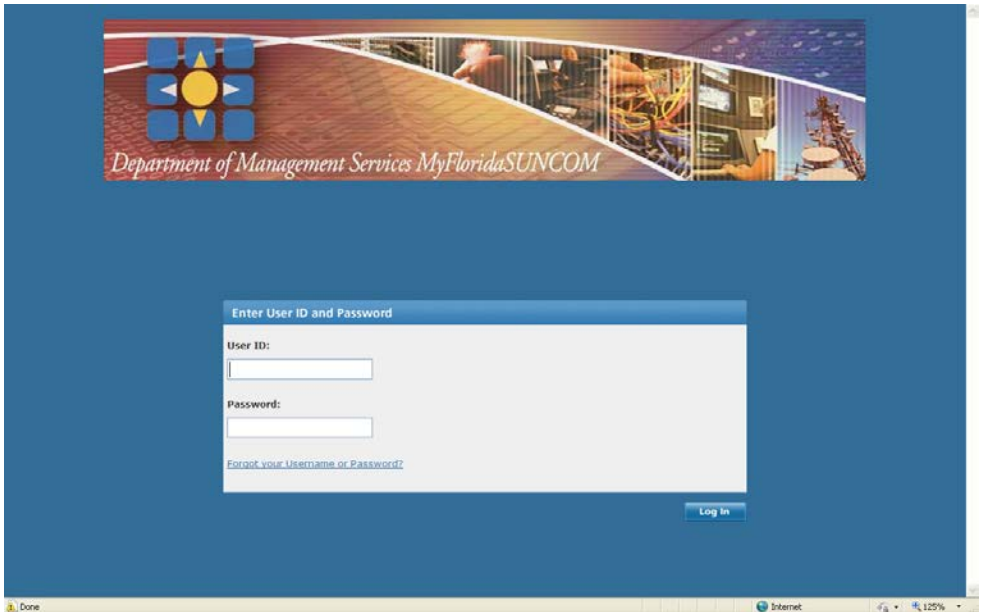


Figure 7—Login Screen

- Tools are located in various locations and interface with multiple systems from multiple contractors.
- Users have access to all tools, but only to devices or interfaces that are providing service to the user.
- Accessible from outside of MyFloridaNet.
- Web-based service using Java scripts.
- Monitors SysLogs, Traps and Polls to devices in the MyFloridaNet regardless of contractor.

The MyFloridaNet Portal is the primary access point to the network management tools provided as part of the MyFloridaNet services. The portal can be accessed via http://portal.mfn.myflorida.com. The portal provides access to tools such as Spectrum, eHealth, NetQoS, Remedy Ticketing System, Router Configurations, Core Router Proxy, and QRadar (the Security Tool). These tools, with sample screen shots, are briefly described below.

- ***CA Spectrum Infrastructure Manager*** – This application provides measurement and alarming on network performance, availability and SLA adherence. (Figure 8)

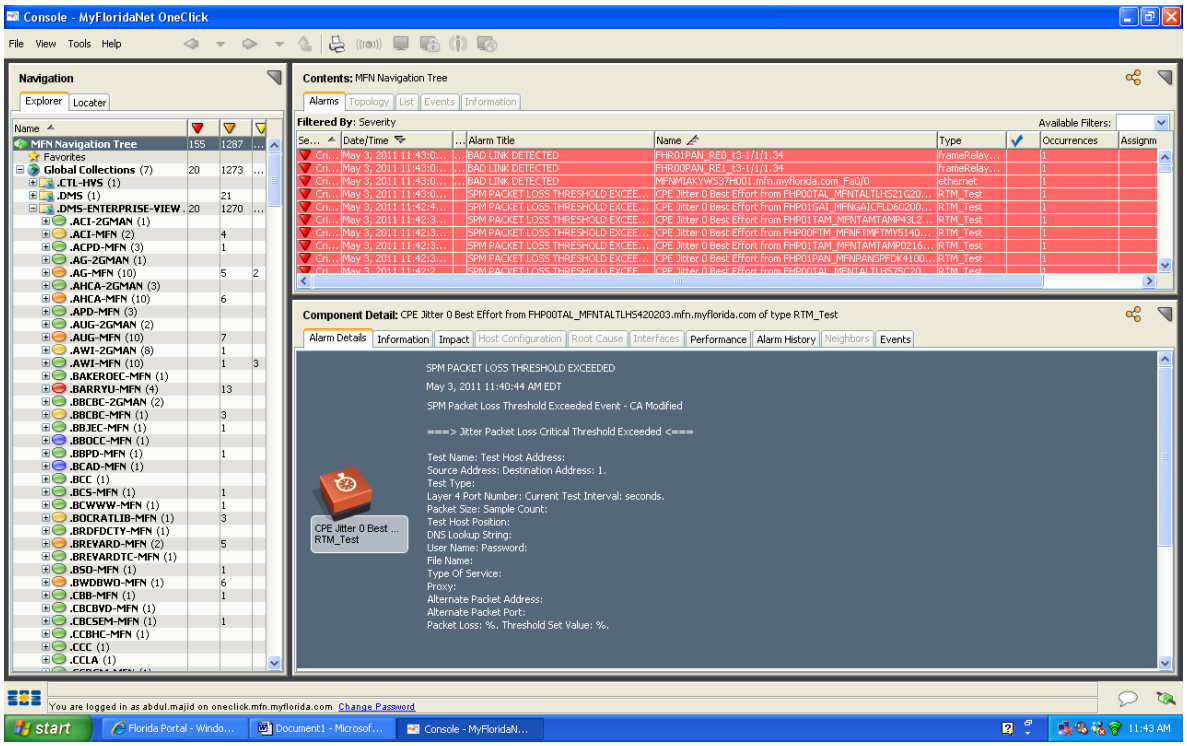


Figure 8—CA Spectrum Infrastructure Manager

The remainder of this page is left blank.

- ***CA eHealth – Network Health Manager –*** This web-based application provides trend and historical reporting on network performance and availability, and performs analysis of key metrics. This tool can be of assistance in detecting and anticipating performance degradations before service quality is jeopardized. (Figures 9 and 10)

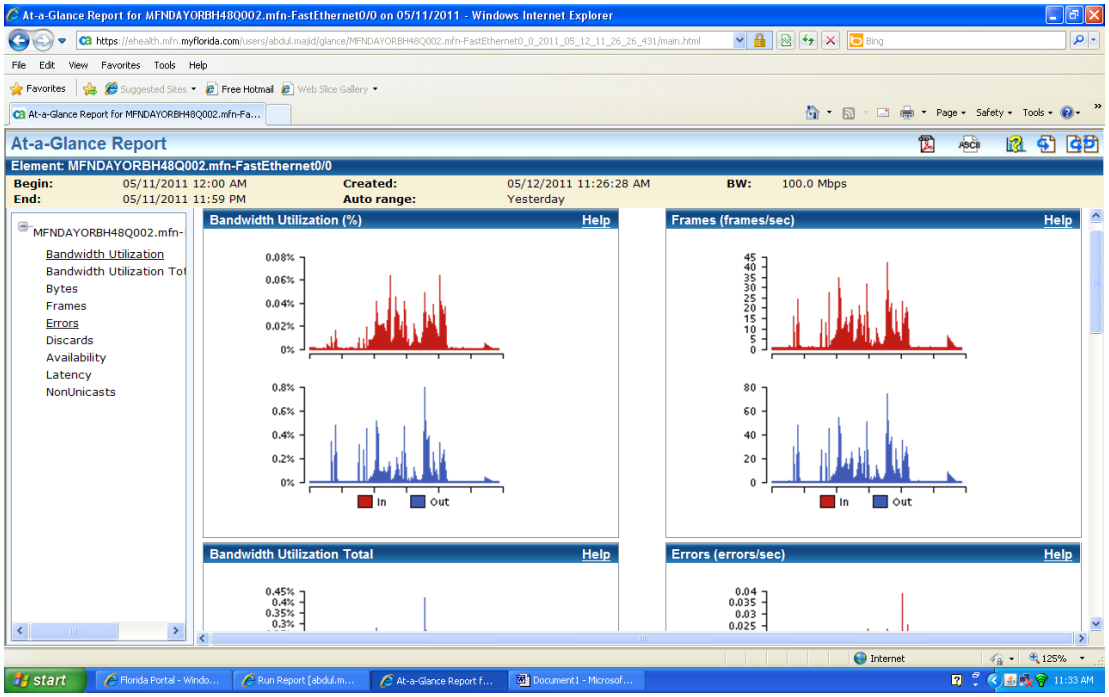


Figure 9—CA eHealth

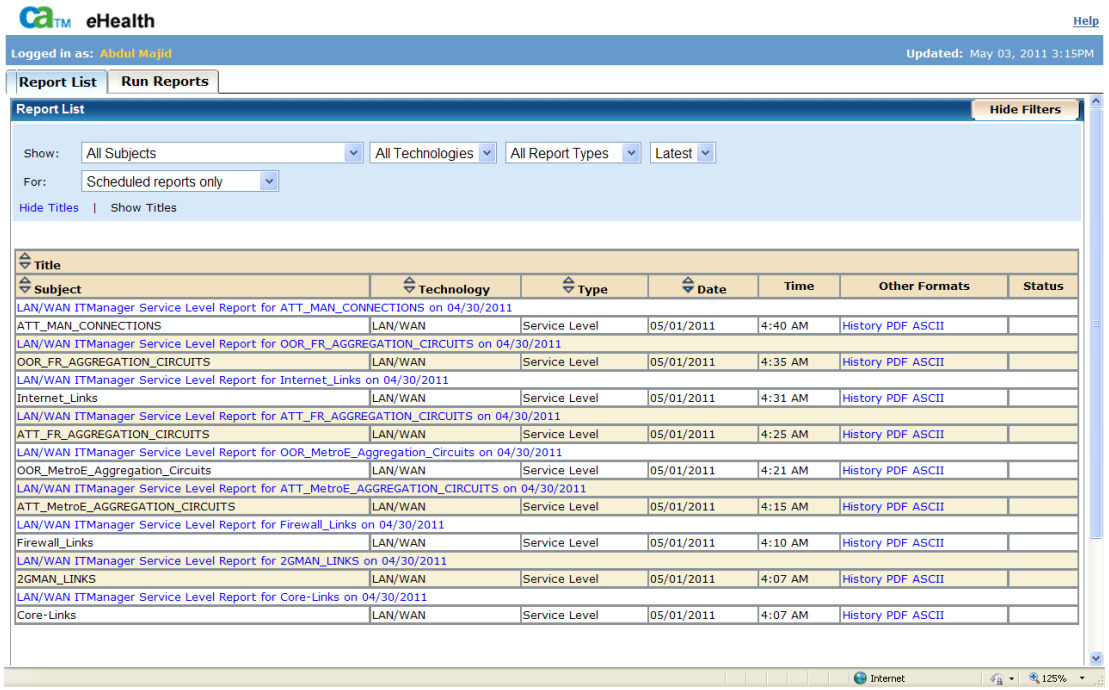


Figure 10—CA eHealth (2)

- ***NetQoS –*** This application provides application-specific network traffic analysis such as data, voice, and video traffic, based on Netflow statistics provided by the MyFloridaNet core routers. (Figures 11 and 12)

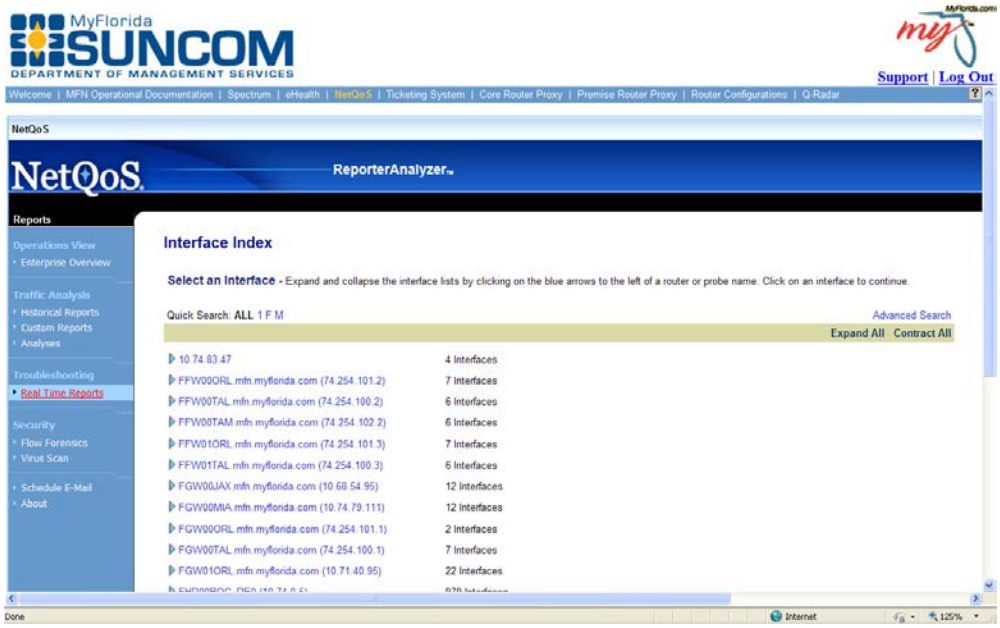


Figure 11—NetQoS

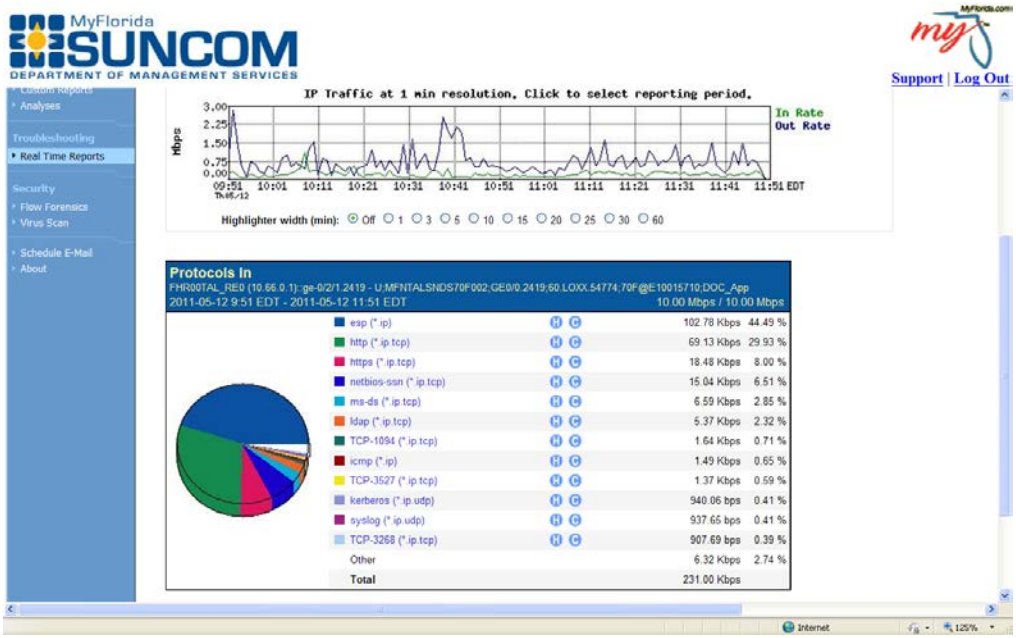


Figure 12—NetQoS (2)

- ***Remedy –*** This application allows users to monitor trouble tickets and search tickets on the Internet from anywhere. (Figures 13 and 14)

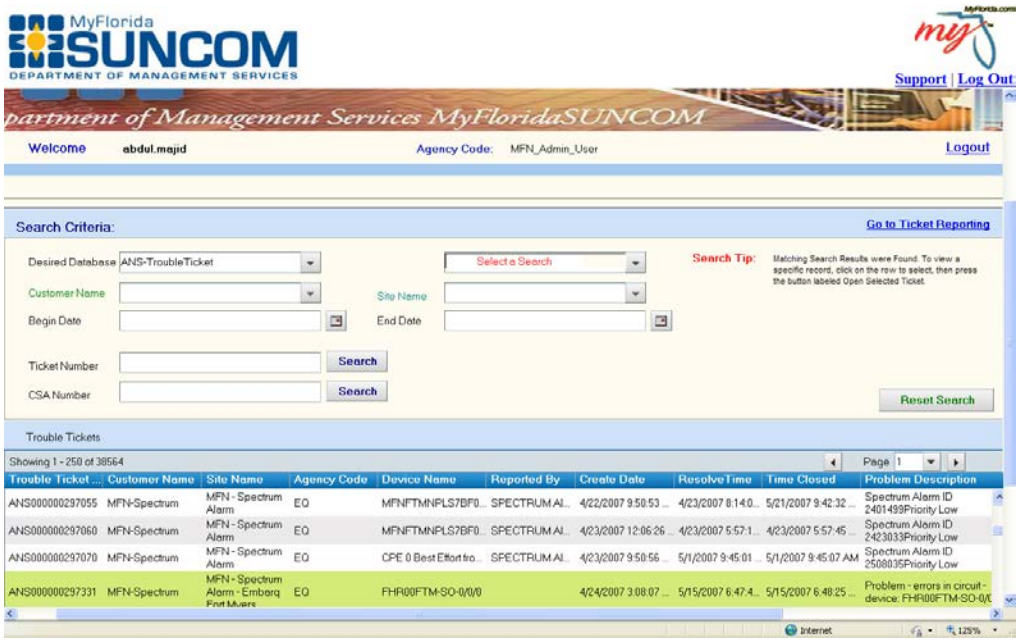


Figure 13—Remedy

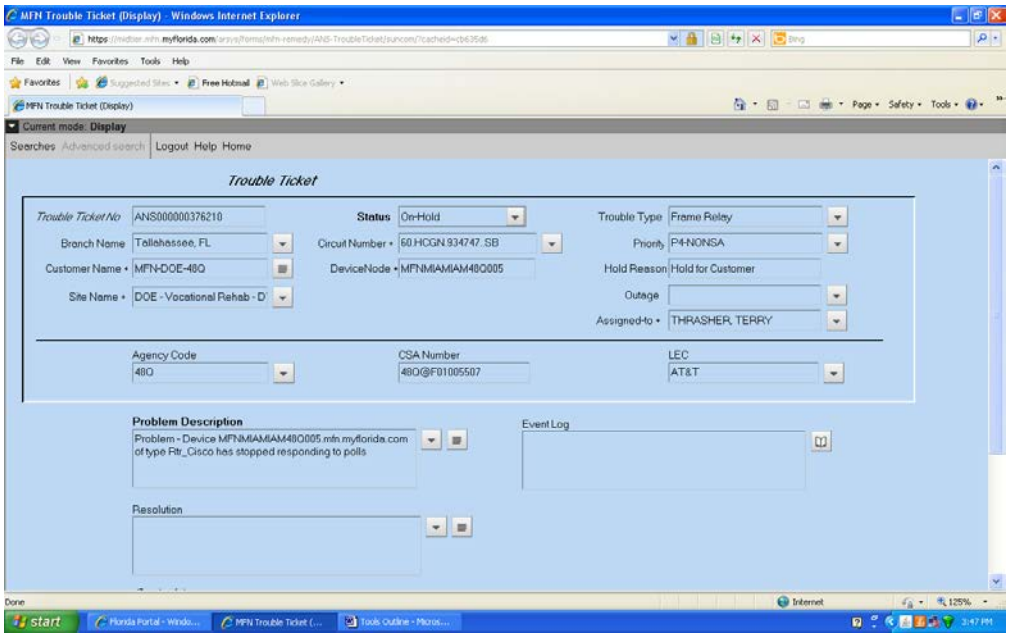


Figure 14—Remedy (2)

- ***Router Configurations*** – Several router proxies provide the capability to view router configurations in MyFloridaNet managed routers. This includes the capability to perform various read-only commands, including ping, trace route, show route table, show interface, etc. Customers are only allowed to see their respective logical or physical interfaces. (Figures 15 and 16)

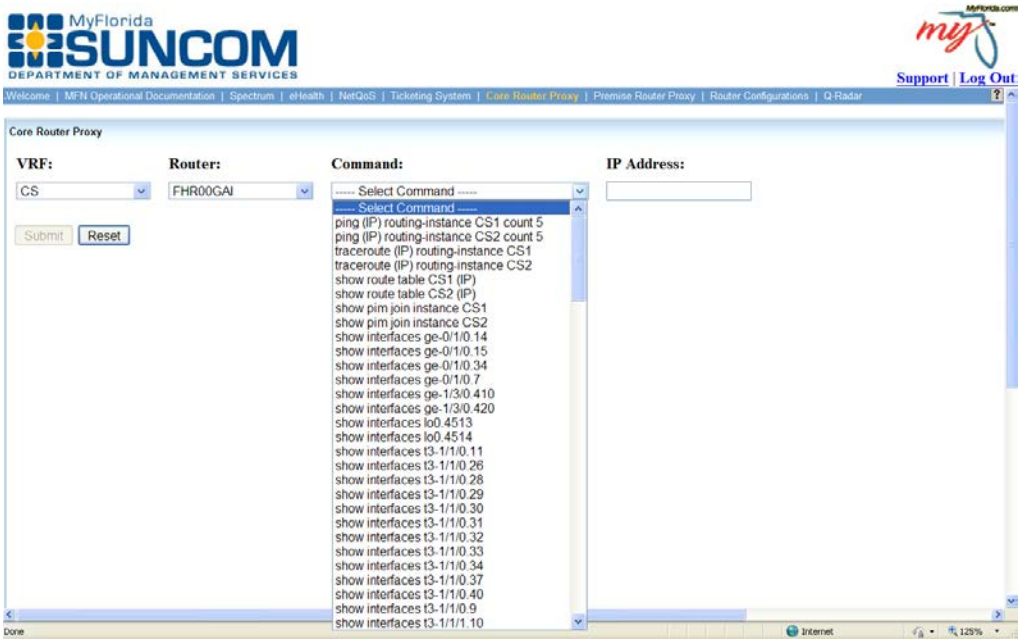


Figure 15—Router Configurations

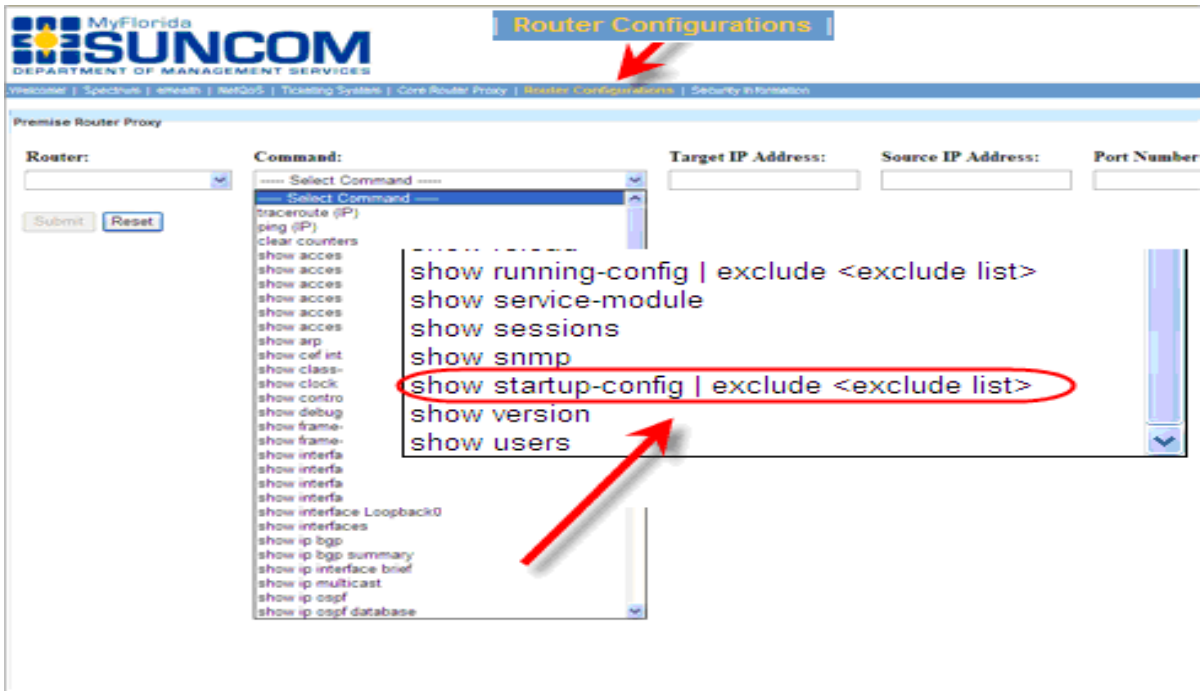


Figure 16—Router Configurations (2)

Return to Index

RANCID manages the MyFloridaNet router configurations, collecting and storing them, and tracking a history of changes. (Figure 17)

Note: Configurations are gathered nightly at 11:00 p.m. and automatically after every configuration is saved to NVRAM. It is imperative that the user's technical resources save the running configurations to the NVRAM when changes are made. This will ensure that changes are captured at the time of the save and archived nightly.

Customers utilizing this tool can access RANCID from the Router Configurations tab in the portal.

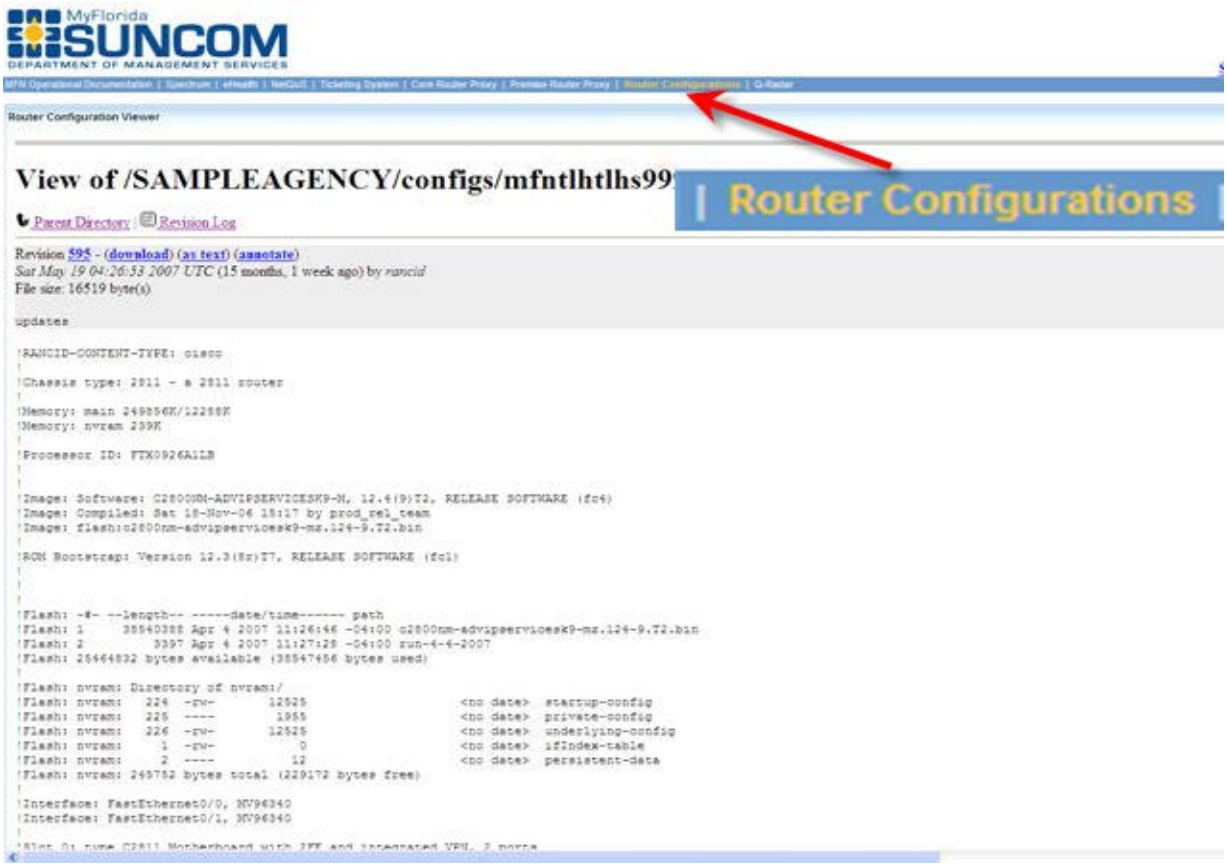


Figure 17—RANCID

The remainder of this page is left blank.

- ***Security Information Manager – QRadar*** – This web-enabled enterprise security information manager (SIM) provides a unified architecture for collecting, storing, analyzing, and querying log, threat, vulnerability and risk related data. The SIM receives statewide NetFlow, intrusion detection system [IDS], and syslogs from core and primary domain controller routers, firewalls, IDS, etc. QRadar correlates all information received and alarms based on severity. All customers who have a security role are granted access to their respective partition. (Figures 18 and 19)

Figure 18—QRadar

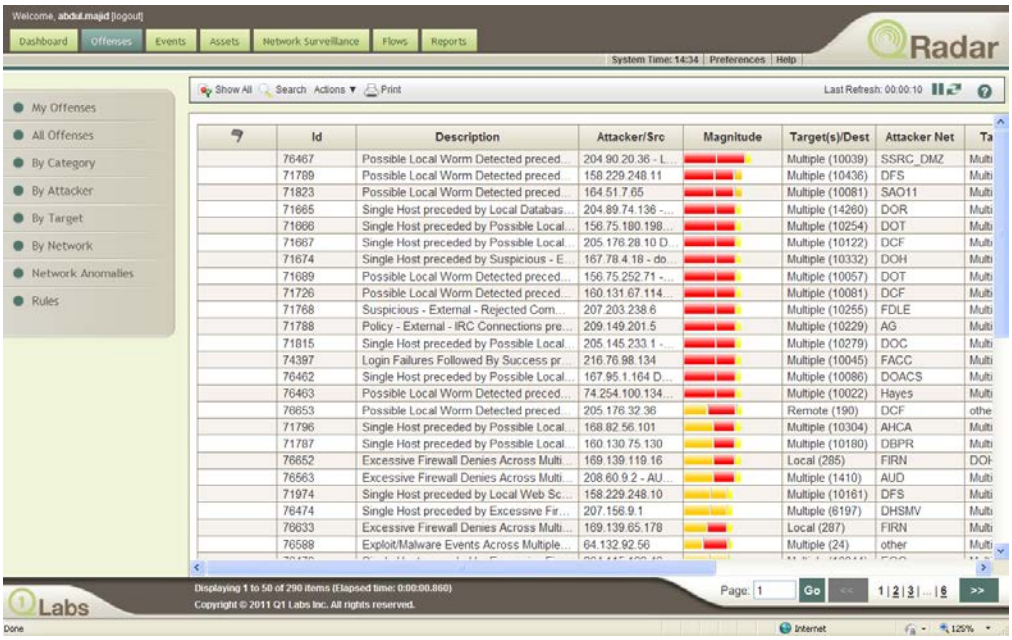


Figure 19—QRadar (2)

4.0.4.2.5 Network Management System Training

Users have access to training for the MyFloridaNet Network Management tools through two approaches:

- Online web-based training
- Local or web-based instructor-led training

Special in-depth classes are held at Department facilities or at agency locations in Tallahassee. If users are remote, web-based live training is supplied if possible. Training agendas are customized according to customer needs. Classes are led by experts involved in installing and maintaining the systems.

The remainder of this page is left blank.

4.1 General Requirements

Respondents shall describe a solution that will meet the requirements. A general logical diagram of the components or functions expected is shown here for reference. (Figure 20) (A large version is included as Exhibit A.) Respondents shall prepare similar diagrams to describe their solution.

The NG-911 Routing Service shall be a NENA i3-compliant system at the core. All ingress or egress to or from the core shall be converted to or from NENA i3 protocols for processing and for transport through the core as required and as specified throughout this document.

The NG-911 Routing Service shall utilize MyFloridaNet for wide-area IP transport. IPv6 shall be utilized exclusively throughout the core for all SIP signaling and media transport. The MyFloridaNet 911 VRF may carry some IPv4 traffic either natively or via tunneling to NG-911 IPv4 interconnection points or between PSAPs for non-NG-911 Routing Service applications. Interconnection with IPv4 networks, where required, shall be via Session Board Controllers or other devices capable of converting the application data streams between IPv4 and IPv6 transport.

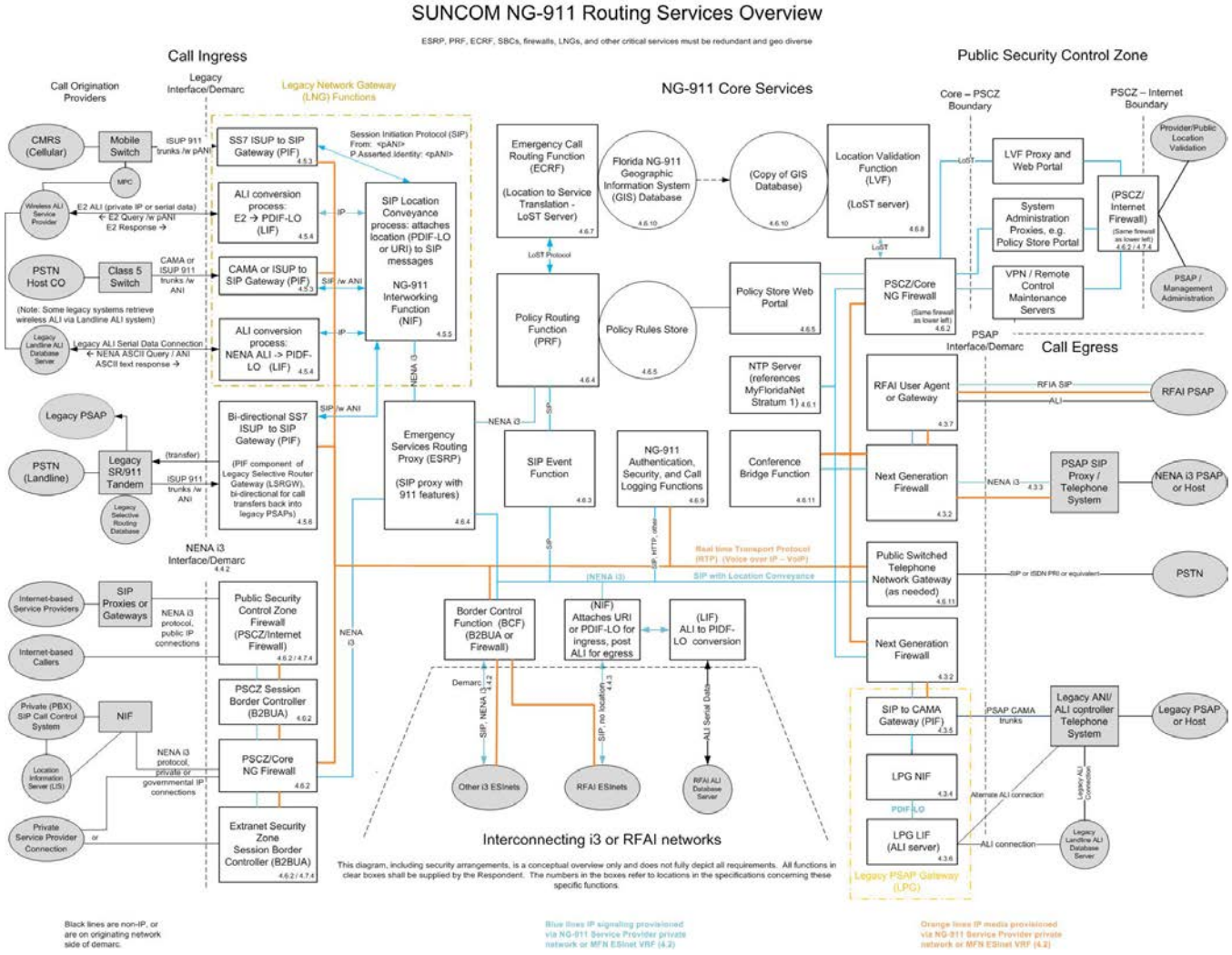


Figure 20—Expected Components or Functions

Return to Index

In addition to these functions, the NG-911 Routing Service shall be divided into distinct security zones. A security zone is an interconnected set of IP subnets within which IP packets may be freely exchanged among connected IP hosts and gateways. Unless otherwise noted, the perimeter of each security zone shall be protected via next generation firewalls, as specified in section 4.3.2, from interconnected adjacent security zones. The diagram in Figure 21 illustrates the relationships among the security zones as described below.

More information on the security of the system is included in section 4.7.4, but is based on making use of multiple security zones as depicted in Figure 21. (A large version is included as Exhibit B).

The remainder of this page is left blank.

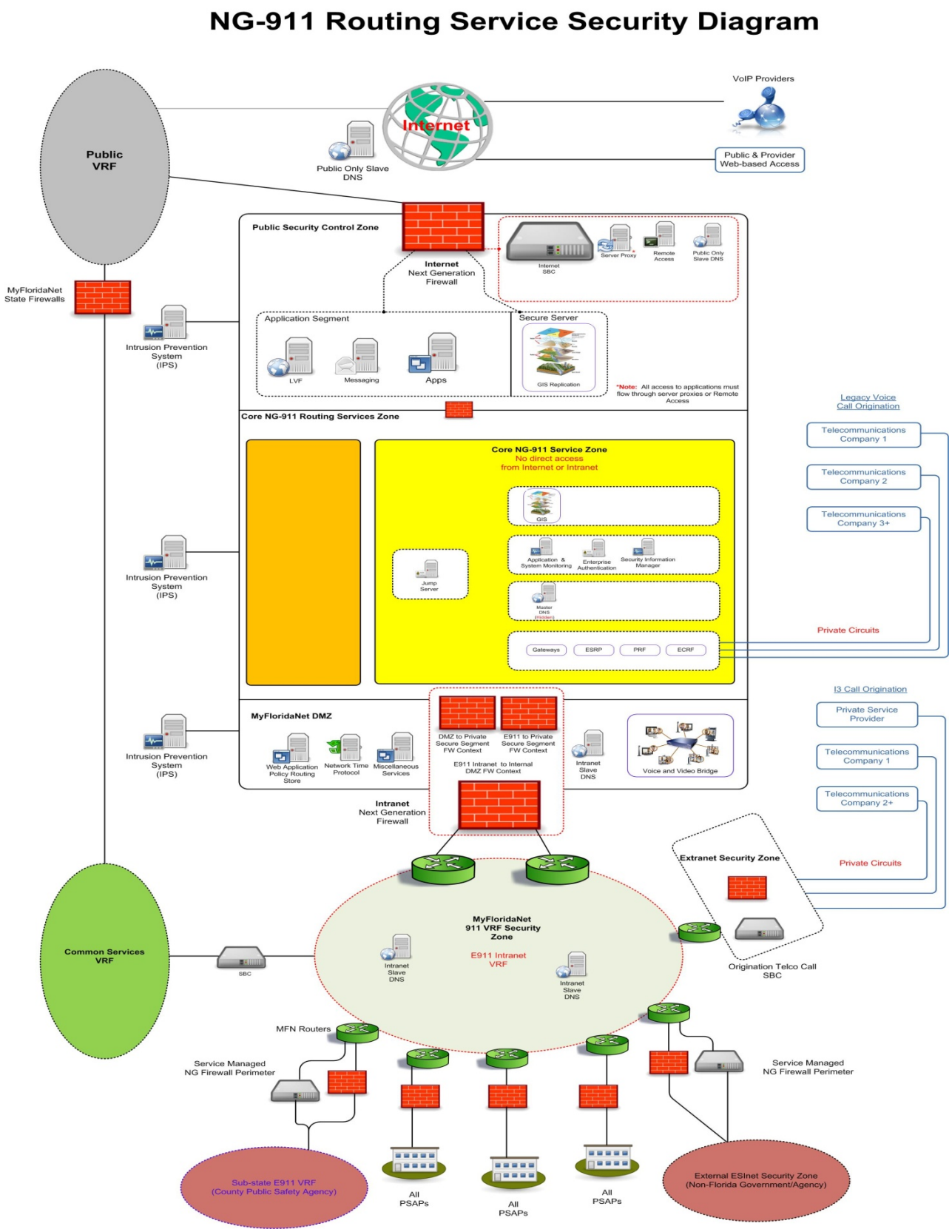


Figure 21—Security Zones Diagram

Return to Index

4.1.1 Respondents shall apply the general guidelines that follow to all answers for the subsequent requirements.

4.1.2 Respondents shall provide detailed information for each requirement that will clearly describe how the Respondent plans to meet the requirement, and shall include diagrams and process flows to demonstrate the Respondent understands and has the ability to meet the requirement. A simple statement that the Respondent can do requirement "X" without the description of how the requirement is satisfied will not be adequate.

Respondents shall disclose the functional deployment scheme in their solutions by providing diagrams, tables, and/or a narrative that shows where the specific functions discussed in subsequent requirements will reside. Example call or data flows between the functional elements shall be included. If a function resides at multiple PSAP sites, then a description of one typical PSAP site may suffice, although site-specific differences shall be noted.

This information will be closely scrutinized to ensure that call and data flows over the NG-911 Routing Service–to-site demarcation and the Emergency Services Routing Proxy (ESRP) inputs are standards-based, and that no critical function utilizes or requires proprietary signaling across these boundaries.

4.1.3 Florida understands that NG-911 is a solution that, with effort, will constantly change to allow for new technologies and services, and is looking for a service-based solution. The Department is committed to providing this service under a philosophy of rapidly accommodating change, and will expect the successful Respondent to be a partner in this process as much as a contractor. Respondents should define the process to be used when adopting new features to include key steps, approvals, and timeframes.

4.1.4 Many types of interconnections of which the Department is aware are listed, but Respondents shall be expected to interconnect with all call origination service providers and all types of PSAP and sub-state ESInets. Not all functions may be captured in this document for these interconnections or functions within the NG-911 Routing Service. Respondents shall identify any other requirements that the Department should consider and list all known potential hidden costs that may not be outlined in this document.

4.1.5 The selected contractor shall use available SUNCOM services such as Internet, telephone access to the public switched telephone system, and long distance services. Respondents shall describe the SUNCOM services required by the Respondent's solution, and shall include sizing estimates, e.g., 10 Mbps of Internet access bandwidth and 46 channels of public switched telephone network (PSTN) primary rate interface access.

4.1.6 To fully understand the Respondent's solution, the Department requires that call flow diagrams be included to demonstrate the process and systems used for various functions within the NG-911 Routing Service. Example diagrams are included in Exhibit C. Respondents shall provide a detailed design plan for all components that make up the service. This design shall show physical, security, and logical diagrams of all functions and devices described in this document.

4.1.7 The Respondent's solution shall comply with open standards as listed in Exhibit I. The most basic requirement is that all emergency calls shall be signaled within the Florida NG-911 Routing Service core utilizing SIP with location conveyance headers and attachments as currently defined by IETF and by NENA 08-003 (*Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3*) specification. All SIP messages in the core shall be transported via Transmission Control Protocol (TCP) using IPv6. Refer to Exhibit I for referenced standards and documents.

4.1.8 The Department seeks Respondents who understand and are fully committed to a SIP-based IP call handling solution, and who understand the architectural impact of SIP and IP networks on that solution. For example, a solution that utilizes core SIP proxies that do not anchor media paths will be preferred over centralized Back-to-back User Agent (B2BUA)-type IP soft switches that require all media paths to be transported to and from central locations. Solutions that simply replace traditional 911 trunks with SIP and VoIP, but which otherwise replicate legacy 911 architecture, are deprecated.

4.1.9 Respondents shall demonstrate specific active involvement of their staff with the NG-911 standards development organizations (SDOs), as well as NENA, involved in the setting of standards for NG-911 and NENA i3.

4.1.10 Respondents shall describe in detail their involvement with the NENA Industry Collaboration Events (ICE).

4.1.11 Respondents shall list all products included in their response that have been tested in a NENA ICE session and the results of that testing within the limitations of the ICE participation agreements.

4.1.12 Respondents shall drive the migration of ECON operators to the proposed NG-911 Routing Service solution, and facilitate the migration of the PSAPs to the NG-911 Routing Service. Respondents shall describe in detail their plan to facilitate the migration of existing 911 services to the NG-911 Routing Service at all interfaces between the Respondent and other ECON operators. ECONs include major incumbent local exchange carriers (ILECs), wireless providers, independent LECs, and government and private telecommunications system operators. The purpose is to accomplish 911 call deliveries that meet the quality and reliability requirements of this document. The plan must make clear the method and order of deployment of the components of the NG-911 Routing Service. This plan shall include a proposed schedule and implementation plan, to include diagrams of the build out, the initial and final call flows, and functions deployed. Respondents shall state the terms, conditions, procedures, or processes for interconnection and exchange of information between other carrier's networks and systems and the Respondent's networks and systems.

4.1.13 The Department is procuring a service, not purchasing equipment, but the successful Respondent shall provide the State of Florida complete visibility into the NG-911 Routing Service. The required visibility includes read-only access to all dedicated component and partitions from ingress to egress, including access to command line interfaces (CLI), graphical user interfaces (GUI), and raw transactional and operational logs. Respondents shall provide an explanation of how they will acquire and deploy all equipment, including servers, displays, Ethernet switches, IP routers, wiring, etc., as required to implement the NG-911 Routing Service. Respondents shall describe whether the equipment used by the Respondent is owned or leased. Respondents shall also state if the equipment is dedicated to Florida or

is shared; and if shared, how it shall be partitioned for the state of Florida's use. Respondents shall describe how the Department will be allowed access to all systems.

4.1.14 NG-911 Routing Service equipment will be located in various areas of the state to include data centers and PSAPs. Respondents shall describe the plan to maintain and service all equipment, to include expected service dispatch to technician on-site times, at all locations including PSAPs. Respondents shall list all other service providers, sub-contractors, and spare equipment locations that are a part of this service.

4.1.15 NG-911 Routing Service critical functions, such as the legacy network gateway (LNG), ESRP, and Emergency Call Routing Function (ECRF), shall be provisioned such that the interruption or failure of any single process instance, the failure of any single component, or the failure or the halting of the hardware platform on which a critical function resides, shall not interrupt the ability of the network to deliver emergency calls from ingress points to call takers. Respondents shall clearly explain how high-availability (99.999 percent uptime) is obtained for each NG-911 Routing Service function. Diagrams shall be used to assist this explanation. See 4.6.1.1 for an example of a satisfactory explanation.

4.1.16 Respondents shall describe how the system is engineered to avoid losing 911 calls in progress and losing new 911 calls being initiated.

4.1.17 A 911 system is always at risk for deliberate or non-deliberate surges in call volume. Respondents shall describe how the call flow traffic design and engineering are used to limit or throttle calls to PSAPs and throughout the system. Respondents shall describe each potential choke point and the normal activity and limits of each point. Respondents shall include the process to change these limits if available.

4.1.18 The NG-911 Routing Service shall not drop a 911 call due to the receipt of an error or other unexpected response, but the NG-911 Routing Service must deliver the 911 call to a human call taker close to the preferred destination as is possible under the circumstances.

4.1.19 Respondents shall review Exhibit D for call volume numbers and develop estimates for sizing the proposed system. Respondents may use 8,100 busy hour 911 calls as a default, but that number is an estimate developed from an estimate of 20 percent of calls per day as a busy hour with an equal distribution each day. Respondents shall describe the methods they use to develop busy hour estimates if different from the default.

4.1.20 The Department requires that all components, systems and interfaces in the response be tested. The Department will review and approve all final test plans, which shall include testing of individual components as well as sub-systems and a full NG-Routing Service test. Testing shall include a minimum period of 30 calendar days after the complete cut-over when the NG-911 Routing Service is live and running normally before acceptance by the Department. Any major failure during this time may require the testing period to be extended. Respondents shall describe the process for the acceptance testing of all components, systems, and interfaces in the response. A sample test plan shall be included in the response.

4.1.21 The NG-911 Routing Service is a full-time service and shall operate 24 hours a day, 7 days a week (24x7). Many activities will be required to be performed outside normal business hours to reduce the impact to

the 911 system and PSAPs. This will require the successful Respondent's staff to be available to perform implementation and maintenance at all hours. Respondents shall not charge overtime for any activities of the NG-911 Routing Service, and shall plan for resources being available 24x7.

4.1.22 Respondents shall include a staffing plan for each project phase (implementation, migration/cutover, and post-migration operations) in the response, which must include the following:

- List of key positions required for each project phase
- The percent of time each week these key personnel are dedicated to the project for each phase
- How the Respondent anticipates personnel requirements may change over time
- List of specific personnel that will fill these key positions and resumes for each person

Respondents shall complete and submit Exhibit E—Staffing Worksheet to identify the staff to support the NG-911 Routing Service. The Staffing Worksheet requires the following information:

1. Description of staff allocations by functional description by percent of time allocated per month and a monthly and quarterly report showing the total headcount and full-time equivalent (FTE).

2. Description of how competence for the proposed service areas will be assured.

To facilitate a simple comparison between staffing levels for the competing responses, Respondents shall complete the staffing tables in the worksheet in response to "1" and "2" below. The tables must include the number of staff expected to participate in the management and technical teams. Table entries should be as descriptive as possible, including fields such as experience level and function (duty or role). The goal is to provide the evaluators with a total staffing picture by FTE.

Each table should allow the evaluators to determine the FTE allocated to the project at least 25 percent of the work week and those allocated below that level. Tables should indicate the distinction between the transitional phases, where the successful Respondent must invest intensive personnel to begin working on the project immediately, and those proposed for the life of the contract.

1. List members and include resumes of the management team that will be used to support all key components of the NG-911 Routing Service, and describe each person's level of experience in managing services for other projects similar to this system. List the extent and percentage of hours that all key staff will be allocated to the performance of work under this solicitation.

2. List members and include resumes of the technical team that will be used to support all key components of the NG-911 Routing Service, and describe each person's level of experience in providing technical services for other projects similar to this system. List the extent and percentage of hours that all key staff will be allocated to the performance of work under this solicitation.

4.1.23 Training on the proposed technology is anticipated in the deployment stages and throughout the life of the project. The Department requires training and related instructional services in order to maintain its expertise with the NG-911 Routing Service and communications systems and tools. Training sessions are for Department staff responsible for the NG-911 Routing Service; County agencies will be invited to

participate. Classes are to be offered tuition free at DMS or County facilities. Instructors must possess advanced knowledge and experience in the topic they present. Respondents shall provide a proposed yearly training plan that outlines the stakeholders and subject of the training on the system. A description of the initial training, follow up training, and annual training on technologies related to the NG-911 Routing Service, including industry topics such as NENA i3 standards, IPv6, security, operational tools, IP multimedia subsystems (IMS) and the equipment utilized in NG-911 Routing Service should be included. The plan must also cover general topics, including research on developing topics in communications and network services. The NG-911 Routing Service Contractor shall be required to update the plan yearly.

4.1.24 The Contractor is also required to pay for State personnel to participate in research on developing topics in NG-911 communications and network services training classes, technology applications visits, conferences, user group meetings, and the like. This training will include travel, lodging, meals, and registration fees, etc. This activity will address NG-911 related topics, to include, but not be limited to: IP, SIP, IMS network infrastructure, NG-911 features/functionality, Disaster Recovery, TE, Network Management, and Performance Management. The annual cost will be capped at $50,000.

4.1.25 This is a service and SLAs will be required. These SLAs shall be based on use of this service and will include monetary penalties for services that do not meet these levels.

4.1.26 All hardware and software shall be managed, tested, and maintained by the successful Respondent. Monthly recurring charges (MRCs) will begin only after full acceptance by the Department.

4.1.27 All data created or acquired under this service, including but not limited to, geographic information system (GIS) base data, rule-sets, routing information, raw logs, and analyzed data shall be the property of the Department.

4.1.28 Respondents shall describe NOC and escalation processes.

4.1.29 Respondents shall demonstrate how they plan to integrate with ECONs that utilize IMS.

4.1.30 The Department requires Contractors to assist Departmental staff in the development and implementation of new services and technologies; proposing options to facilitate changes, upgrades and new features. Respondents shall include a technology refresh plan that outlines the commitment for on-going services and technology refresh for the tenure of their involvement with the NG-911 Routing Service.

a. Respondents shall state a mechanism whereby they commit to a framework of costs or cost models, and timeframes under which they will meet these newly defined service needs and respective service delivery windows. Technology refresh must span all NG-911 Routing Service components (e.g., access, daily operations, billing, etc.).

b. Core and customer premise equipment (CPE) software refresh will commence as needed to satisfy SLAs. Core software refresh is to ensure service levels are continually met, that full successful Respondent support is continuously available, and the support of new features is

available. The core software suite will be refreshed (at Department's option) as long as the result will not impact these objectives.

c. NG-911 Routing Service hardware refresh will commence as needed to satisfy SLAs. The Department requires current hardware. All features and functionality will be supported completely for the initial term and any renewal term of the contract. Responses shall define their strategy, including a specific timeframe, for providing upgrades when the equipment is stated as end-of-sale, end-of-life, end-of-service, end-of-support, or any other deadlines terminating use or serviceability of the equipment by the original equipment manufacturer.

4.1.31 The successful Respondent shall establish a technology refresh fund of $100,000 per year. Respondents shall describe the process used to accomplish technology refresh of the proposed NG-911 Routing Service, and the costs associated with this refresh.

4.1.32 The NG-911 Routing Service core infrastructure shall be implemented and maintained for the exclusive use of the State of Florida; dedicated and private devices or partitions. Core components such as routers, links, DNS, firewalls and intrusion prevention systems (IPS) are not to be used to support other service provider clientele. Respondents shall clearly define strategies used to provide dedicated and private components.

4.1.33 Respondents shall provide a detailed design plan for DNS. The DNS system shall be designed to meet the high availability and high reliability needs of the NG-911 Routing Service, and must interoperate with the MyFloridaNet DNS system. The DNS design must be consistent with MyFloridaNet requirements. Specifically, master NG-911 DNS are required in the Core NG-911 Routing Service security zone. Access to these master DNS shall be restricted to processes located in the Core security zone and to slave DNS that are located in security zones outside of the Core security zone. All processes outside the Core security zone shall utilize slave DNS.

4.1.34 In addition to the requirements listed above, Respondents should highlight any distinguishing aspects of their service to be considered during the evaluation for the NG-911 Routing Service.

The remainder of this page is left blank.

4.2 IP Transport Requirements

The proposed NG-911 Routing Service solution shall utilize the enterprise IP infrastructure service operated by the Department, known as MyFloridaNet.

MyFloridaNet is a carrier class statewide MPLS network featuring a fully redundant and diverse synchronous optical network (SONET) backbone with 10 Gbps links. All backbone and access routers used to deploy MyFloridaNet are dedicated to MyFloridaNet. The MyFloridaNet backbone is designed for 99.999 percent availability. MyFloridaNet is fully managed and monitored.

If a proposal has special IP transport requirements or a Respondent has compatibility issues with the use of MyFloridaNet for IP transport, but the proposal otherwise ranks highly during the request for proposal (RFP) evaluation process, the Department, at its sole discretion, may elect to satisfy such requirements or may negotiate with the Respondent in an attempt to arrive at a satisfactory solution. If no such solution can be found, the Department reserves the right to reject the proposal and select another proposal.

The IP transport requirements are found on the following pages.

4.2.1 The successful Respondent shall establish a business and a working relationship with the Department for provisioning IP connections, for trouble ticket processing, and for other wide area network (WAN) IP infrastructure needs as required. Respondents shall describe where they have similar relationships.

4.2.2 MyFloridaNet shall be used to provide the wide-area IP transport for the NG-911 Routing Service. Respondents shall thoroughly familiarize themselves with the technical specifications of MyFloridaNet, and shall disclose in their proposals any potential impact to the proposed solution from the requirement to use MyFloridaNet. If Respondents have technical requirements for IP transport that are not fulfilled by MyFloridaNet, such requirements shall be clearly stated in the proposals. The Department may entertain helping to overcome any hurdles, but will not eliminate MyFloridaNet as the IP transport.

4.2.3 The proposed NG-911 Routing Service solution shall use MyFloridaNet to transport all wide-area NG-911 IP traffic between PSAPs, data centers, public safety responders, and any successful Respondent-supplied NG-911 sites, including all NG-911 signaling and voice paths within the state of Florida. All connections to PSAP sites and/or to sub-state ESInets shall be provisioned through MyFloridaNet. Respondents shall provide a network diagram of these connections, including any out-of-state end points.

4.2.4 MyFloridaNet shall be used to provide the IP transport for the NG-911 Routing Service. To provide a baseline for comparison of the proposed solutions, Respondents shall describe IP transport requirements for the proposed solution, to include, at a minimum, bandwidth, latency, jitter, and packet loss for each connection, to include primary and backup routes.

4.2.5 MyFloridaNet uses an established window for maintenance, and includes contractors on its notification list. The successful Respondent must avoid maintenance activities during MyFloridaNet maintenance windows to avoid conflict, and, regardless, must coordinate activities with MyFloridaNet. Respondents

shall describe the process or design used to manage maintenance outages on the system and MyFloridaNet, to include notifications to all stakeholders.

4.2.6 MyFloridaNet prefers to provide the IP routers for the PSAP, sub-state ESInet borders, and Core sites within Florida. MyFloridaNet could also provide IP routers for outside the state if requested. Respondents shall describe the quantity and functions required for the proposed NG-911 Routing Service solution.

4.2.7 If the Respondent requires additional IP routers or IP devices or services, these shall be provisioned as follows:

- IP devices shall accept and route IPv6 packets.
- All services shall support IPv6 interfaces.
- IP devices on MyFloridaNet shall comply with the MyFloridaNet IP addressing standards.
- Network address translations (NATs) shall not be used on the WAN.
- Elements connected to the NG-911 Routing Service shall not be referred to by their IP address, but rather through a hostname using DNS, with a standard naming convention that complies with MyFloridaNet naming conventions.
- All CPE shall utilize the MyFloridaNet configuration template and follow the current E911 naming standards.
- Statically assigned IP addresses shall be limited to network infrastructure (routers and switches) and core NG-911 Routing Service processes. Static IPv6 prefixes shall never be assigned.
- Dynamic Host Configuration Protocol (DHCPv6) shall be implemented to provide managed central control over IP addresses and other services.
- IP routers shall provide QoS utilizing Priority queuing and Differential Services and shall be able to classify all voice, video, and other multimedia traffic in the MyFloridaNet Emergency Voice Queue.
- Routers shall provide dynamic VPN.
- Routers shall provide BGP.
- Authentication and Monitoring shall be provided, as specified in sections 4.6.1 and 4.7.2.
- All activities shall log to the SIM system, as specified in section 4.7.4.12.
- Routers shall provide bidirectional forwarding detection (BFD) both on WAN and local area network (LAN) interfaces.
- Routers shall provide Hot Standby Router Protocol (HSRP).
- Routers shall generate 1:1 Sample Netflow.
- MyFloridaNet IP devices shall provide a method to demonstrate SLAs measuring IP performance.
- All 911 or emergency services shall be implemented with BFD.

4.2.8 The NG-911 Routing Service naming conventions and IP addressing must be coordinated with MyFloridaNet guidelines to utilize state addresses for public, private, and other security zones. A copy of the naming conventions and the IPv6 addressing plan may be requested from the Department under non-disclosure agreements. Respondents shall submit an addressing plan or strategy to include IPv4 public address requirements (e.g., as used in the public security control zone [PSCZ]).

4.2.9 Telecommunications Service Priority (TSP) Service: It is recommended that 911 and emergency services customers order the MyFloridaNet TSP option. The TSP program provides national security and

emergency preparedness users with priority authorization of telecommunications services that are vital to coordinating and responding to crises.

4.2.10 Quality of Service: 911 and emergency services customers must have their voice traffic placed in the EMERGENCY_VOICE QoS Queue. These connections must still adhere to the normal QoS limitations as detailed in the QoS section of the MyFloridaNet user guide.

4.2.11 Design Meetings: All 911/emergency services networks should have pre-sales design meetings conducted with engineering and implementation teams.

4.2.12 Demarcation and Power: 911/emergency services customers should ensure that all their communications equipment is provided with redundant backup power. Customers should also familiarize themselves with MyFloridaNet demarcation points for WAN circuits and LAN handoffs.

4.2.13 Naming Convention: Customer devices will use "911" as the network identifier to identify 911 sites/devices easily. The majority of non-911 devices use "MFN" as the network identifier. A "911" network identifier example follows for Dade County in Miami: 911MIAMIAMN56001.mfn.myflorida.com --- (911)(LATA)(4-letter city)(3- Character agency ID)(3-digit device ID). A complete description of the naming conventions as required by the Department is available under non-disclosure as specified in 4.2.8 above.

4.2.14 BFD: All 911 or emergency services shall be implemented with BFD. BFD is a media and protocol independent liveliness detection mechanism used to detect link failure in situations where the existing failure detection methods are either not present or do not offer fast enough convergence times. On MyFloridaNet, the number of BFD sessions per Core router is limited, so BFD is only used for emergency services, public safety, or data centers and only when there are applications with very low tolerance to packet loss/convergence times such as VoIP.

In addition to the requirements listed above, Respondents should highlight any distinguishing aspects of their service to be considered during the evaluation for the NG-911 Routing Service.

The remainder of this page is left blank.

4.3 Individual PSAP and Hosted CPE Interconnection Requirements

This section describes the requirements for the system to interconnect with the PSAPs that choose to connect. Three types of PSAPs are expected to interconnect, as described in Table 3.

Table 3—PSAP Environments

Environment	Interface to ESInet
Stand-alone/Hosted PSAP Automatic Number Identification/Automatic Location Identification (ANI/ALI) controller (Centralized Automatic Message Accounting [CAMA])	Next generation firewall, legacy PSAP gateway
Stand-alone/Hosted PSAP supporting i3	Next Generation Firewall, SIP interface
Stand-alone/Hosted PSAP supporting Request for Assistance Interface (RFAI)	Next Generation Firewall, Request for Assistance User Agent (RFAUA), NG-911-specific Interwork Function (NIF)/Location Interwork Function (LIF) gateway, SIP interface

The remainder of this page is left blank.

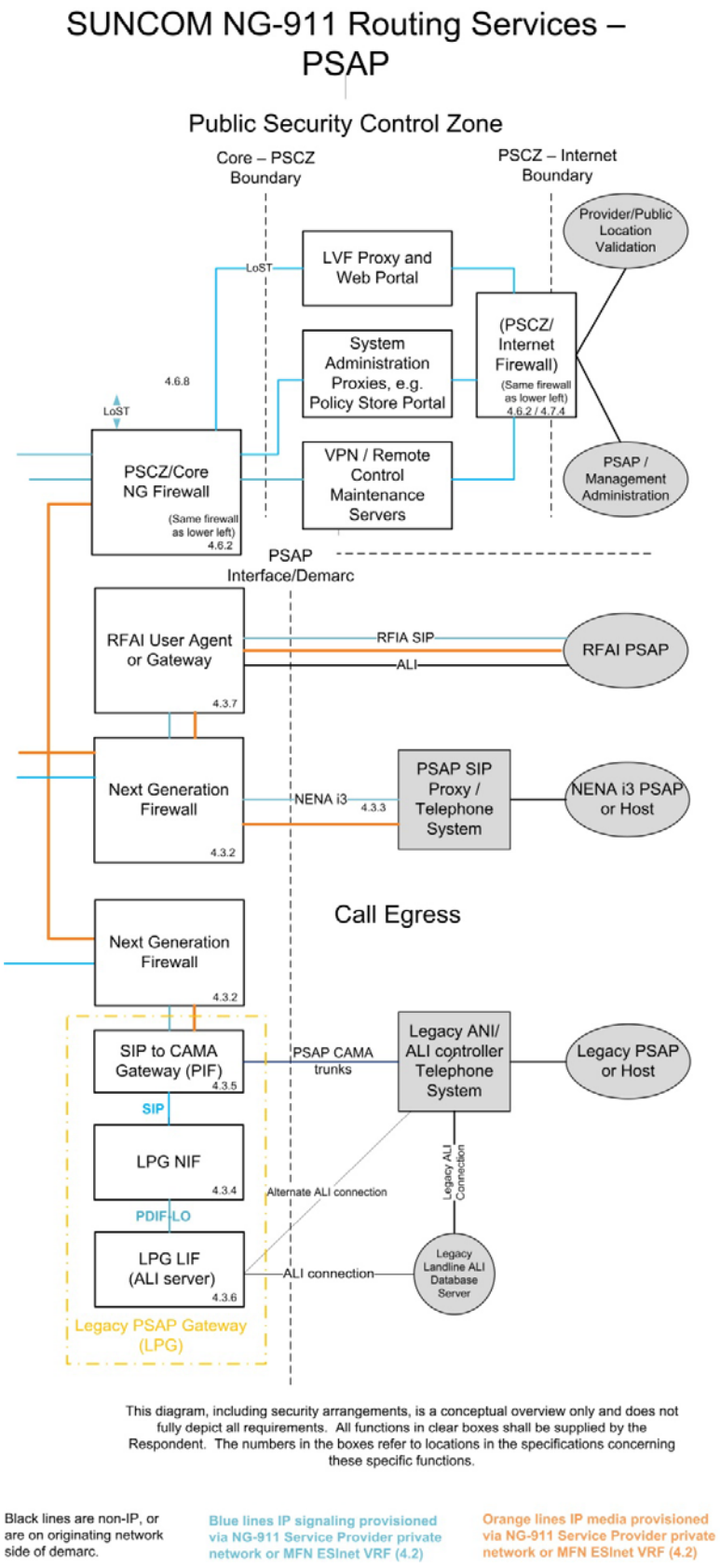


Figure 22—PSAP Interconnections

Return to Index

4.3.1 General PSAP Interconnection Requirements

4.3.1.1 Respondents shall provide an NTP service that complies with the security arrangements specified in 4.7.4, by which PSAPs can synchronize their time in accordance with RFC 5905 (June 2010) for all devices in the PSAP and connected to the system.

4.3.1.2 Many but not all PSAPs will require redundant connectivity to the NG-911 Routing Service functions. MyFloridaNet will provide the transport, but the successful Respondent may require additional equipment at the Core or at a PSAP. The system shall provide the capability for redundancy for network paths and network devices as described in section 4.2. (All PSAPs may not require last mile redundancy at initial deployment.) Respondents shall provide two options for PSAP connectivity for single and redundant connections initially, and shall describe the process required for a single connection PSAP to install redundant connectivity in the future.

4.3.1.3 Diversity shall be accompanied by an automatic failover technology of the proposed NG-911 Routing Service so that a new path can be found through the network in the event one path fails to secure system reliability.

4.3.1.4 The physical network layers shall be physically diverse and provide multiple paths through the network over which IP communications can occur.

4.3.1.5 The NG-911 Routing Service shall use the SIP header and Presence Information Data Format – Location Object (PIDF-LO) formats as listed in section 4.3.3.

4.3.1.6 Respondents shall state their bandwidth requirement for the NG-911 Routing Service per answering position and per active 911 call—assuming a voice call in progress using G.7.11 as a minimum on initial deployment. The NG-911 Routing Service solution shall support bandwidth growth at each site to at least double the initial requirements by adding or using faster facilities, but without replacing major components, such as Core or on-site routers.

4.3.1.7 The NG-911 Routing Service shall provide voice service at the level of the current legacy 911 system initially, but is expected to be used for text and video in the future. This is an open timeline. Respondents shall provide an estimated timeline and bandwidth requirements for introducing this additional media into the NG-911 Routing Service.

4.3.1.8 Respondents shall provide a table to illustrate the required bandwidth of their solution. It is anticipated that the minimum bandwidth to a site shall be at least 1.5 Mbps, but Respondents shall describe smaller bandwidths and any economic feasibility to the Department to use them. Table 4 provides an example.

Table 4—Sample Bandwidth Table

Typical Bandwidth Size	Number of Positions, and Calls
DS-1	Up to XX Positions, and XX Calls
DS-3	Up to XX Positions, and XX Calls
10 Mbps	Up to XX Positions, and XX Calls

4.3.2 Next Generation Firewall

A firewall is a dedicated appliance and should be positioned as a protective device between the hosted system, PSAPs, and other networks, including the NG-911 Routing Service. This provides an outer defensive perimeter for malicious calls or denial of service (DoS) attacks from the PSAP to the NG-911 Routing Service or another PSAP. The firewall inspects ingress and egress traffic running through it.

4.3.2.1 Respondents shall provide a firewall at the interconnection point to any other network such as a PSAP. Respondents will deploy these in a templated fashion protecting the NG-911 Routing Service and other connected entities from PSAPs, call origination providers, sub-state ESInets, and any other outside connection. The data centers hosting the NG-911 Routing Service equipment shall have a firewall to protect the highest security zone where the ESRP and other Core components reside. This is described in the security section. At a minimum, these firewalls shall provide/perform the following functions:

- Application and network layer protection and scanning
- Detection of unusual incoming IP packets that may then be blocked to protect the intended receiving user or network
- SIP aware
- Prevent distributed denial of service (DDoS) attacks; destination-specific monitoring, regardless of the source address, may be necessary
- Adhere to the default deny principle
- High-availability and reliability based on active-active or active-standby configurations
- High performance architecture
- Application identification
- Application protocol detection and decryption, e.g., identify the application protocol, decrypt it, analyze it, and encrypt
- Application protocol decoding, e.g., determine whether the initial protocol detected is the legitimate application or another application pretending to be the real one
- Application signatures, e.g., use context-based signatures to correctly identify the application regardless of port and protocol
- User identification
- Proactive threat prevention
- Stream-based virus and spyware scanning
- Vulnerability attack protection (IPS)
- Uniform resource locator (URL) filtering
- File and data filtering
- Policy control
    - Allow or Deny
    - Allow by scan for exploits, viruses or other threats
    - Allow based on groups, users, or a schedule
    - Policy-based forwarding
    - Allow certain application functions

4.3.2.2 The firewall shall have a mechanism such that malware definitions and patterns can be easily and quickly updated by a national 911 Computer Emergency Response Team (CERT) or other managing authority. Respondents shall describe the process and authority used to accomplish this.

4.3.2.3 Respondents proposed NG-911 Routing Service shall provide heuristics, e.g., if any application eludes signature-based approach, behavioral analysis is applied on applications causing problems such as the ones that use proprietary encryption. Respondents shall describe the engine used to perform this function. Respondents shall describe the process used to keep this function current with the industry.

4.3.2.4 Firewalls shall provide the capability to receive and update 911 malicious content (NMC) filtering automatically for use by federated firewalls in protecting multiple disparate networks (Deep Packet Inspection). Respondents shall describe the processes and services used to accomplish this.

4.3.2.5 Firewalls shall be configured using MyFloridaNet templates and use MyFloridaNet naming conventions. Respondents shall describe the method for policies to be reviewed and approved by the Department on a recurring basis.

4.3.3 PSAP Interface: SIP

All 911 calls entering the NG-911 Routing Service are SIP-based. Gateways, if needed, are outside of, or on the edge of, the NG-911 Routing Service. Implementations are cautioned to be "strict in what you send, and liberal in what you accept" with respect to SIP signaling elements. It is not acceptable to drop a 911 call just because it does not meet some standard detail if it is reasonably possible to process the call anyway.

4.3.3.1 All SIP User Agents (UAs) and SIP Proxies supplied by the successful Respondent shall comply with the requirements of IETF RFC 3261. All SIP UAs and SIP Proxies shall also comply with the requirements of any documents that are referenced by RFC 3261, where those additional documents apply to the proposed solution.

4.3.3.2 Further, all SIP components that participate in the SIP signaling for the delivery of emergency calls, as explicitly labeled on the Florida NG-911 Logical Diagram as “NENA i3,” shall comply with the requirements of NENA document 08-003. These components shall also comply with the requirements of any documents that are referenced by NENA 08-003, where those additional documents apply to the proposed solution.

4.3.3.3 It is important for the Respondent to understand it is also a requirement to interconnect with IP-based sub-state emergency call networks and PSAPs that conform to the Alliance for Telecommunications Industry Solutions (ATIS) RFAI as specified in document ATIS-0500019.

4.3.3.4 While RFAI also requires compliance with RFC 3261, RFAI does not support the SIP location conveyance features of NENA i3, but utilizes legacy 911 ALI systems. A solution to this RFAI interoperability requirement could be based on LNG/legacy PSAP gateway (LPG)-like NIF and Protocol Interworking Function (PIF) functions that convert between legacy ALI and the PDIF-LO and which post ALI or PDIF-LO records or documents in servers for subsequent queries via ANI/pseudo ANI (pANI) or via i3 location-by-reference, as applicable. However, Respondents may propose alternate solutions provided they satisfy the overall intent of a fully NENA i3-compliant set of core services and can successfully interoperate with RFAI sub-state systems or PSAPs as required herein.

4.3.3.5 Of particular concern are 911 calls that originate from any source, including NENA i3-compliant or RFAI-compliant sources, which are converted and transported over the NENA i3-compliant core network, and which may then be subsequently transferred or directly delivered to an RFAI destination. The NENA i3 specification does not necessarily provide means to transport all information required by RFAI through an i3 network. Respondents are advised that the Department will closely examine proposals for their ability to satisfy the RFAI interoperability requirement in a number of scenarios. It will be in the best interest of Respondents to carefully and fully explain their proposed solution via narrative and diagrams.

4.3.3.6 Respondents shall explicitly comply with the requirements below if they extend or expand on the requirements of RFC 3261 or NENA 08-003.

4.3.3.7 All SIP components must accept and receive SIP messages transported via TCP in addition to User Datagram Protocol (UDP). (Different IP port numbers may be used for TCP and UDP transport.)

4.3.3.8 SIP elements in the NG-911 Routing Service shall support the History-Info header and the associated Reason header. Elements that retarget a call shall add a History-Info header indicating the original intended recipient, and the reason why the call was retargeted.

4.3.3.9 All SIP endpoints (UAs) in the NG-911 Routing Service shall support the SIP REFER method and the SIP Replaces: header. This requirement is to ensure the call transfer/conference bridging features described in section 4.6.11 are supported. (Note that the design specifications for the system require that all SIP calls originating from the public Internet traverse a B2BUA session border controller [SBC]. This SBC shall provide "Replaces" support. If other interconnecting systems do not satisfy this requirement, they shall be interconnected to the NG-911 Routing Service via an SBC.)

4.3.3.10 All call handling elements shall support media using Real-time Transport Protocol (RTP) (RFC 3550). Each SIP session initiation message or response shall describe the media the UA is capable of supporting using Session Description Protocol (SDP) (RFC 4566 [14]) in the body of the message.

4.3.3.11 At a minimum, all UAs in the ESInet shall support g.711 mu-law and a-law. Note: It is recommended that Adaptive Multi-rate (AMR), AMR-Wideband (AMR-WB), Enhanced Variable Rate Codec (EVRC), EVRC-B, EVRC-Wideband (EVRC-WB), and EVRC-Narrowband-Wideband (EVRC-NW) also be supported. Respondents shall describe all other coder-decoders (CODECs) supported by the proposed system.

4.3.3.12 At a minimum, all UAs in the ESInet shall support H.264/MPEG-4 video. Respondents shall describe all other CODECs supported by the proposed system and describe how video will be implemented.

4.3.3.13 At a minimum, all call handling elements in the NG-911 Routing Service shall support Framework for Real-time Text over IP using SIP (RFC 5194). Respondents shall describe all other text protocols supported by the proposed NG-911 Routing Service and describe how text will be implemented.

4.3.3.14 PSAPs shall be capable of receiving calls from Telecommunications Devices for the Deaf/Teletypewriters (TDD/TTYs). Transcoders shall be compliant with RFC 5369.

4.3.3.15 Non-human initiated calls presented to the NG-911 Routing Service shall be signaled with a SIP MESSAGE method containing a CAP message, and may be wrapped in an Emergency Data eXchange Language – Distribution Element (EDXL-DE) wrapper. The <area> element of the CAP message shall be copied, in PIDF-LO form, in a Geolocation header in the MESSAGE container. The CAP message shall be in the body of the MESSAGE, with MIMEtype application/common-alerting-protocol+xml. A digital signature shall be included in the CAP message

4.3.3.16 All SIP Proxies should be capable of using Transport Layer Security (TLS) to encrypt SIP messages to/from explicit SIP targets.

4.3.3.17 SIP signaling within the ESInet shall be TCP. Fragmentation and reassembly shall be supported by all NG-911 Routing Service elements. Persistent TLS connections between elements that frequently exchange SIP transactions shall be supported.

4.3.3.18 Media streams for voice, video, and text shall be carried on RTP over UDP.

4.3.3.19 All SIP elements shall implement overload control mechanisms.

4.3.4 PSAP Interface: LPG (NG-911-specific Interwork Function [NIF] Subcomponent)

The NIF component of the legacy PSAP gateway functional element is expected to provide special processing of the information received in incoming call setup signaling to facilitate call delivery to legacy PSAPs; to assist legacy PSAPs in obtaining the necessary call back and location information; and to support feature functionality currently available to legacy PSAPs, such as call transfer and requests for alternate routing.

4.3.4.1 The NIF shall perform the functions described in NENA 08-003 (*Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3*) and maintain the system in coordination with the evolving NENA i3 standards. The NIF shall accept SIP signaling associated with emergency calls.

4.3.4.2 The NIF shall perform a mapping from the non-dialable or non-North American Numbering Plan (NANP) call back information to a locally-significant digit string that can be delivered to the legacy PSAP via traditional multi-frequency (MF) or Enhanced MF (E-MF) signaling. The locally significant digit string delivered to the PSAP shall be of the form NPD/NPA-511-XXXX or as obtained from the Federal Communications Commission (FCC)-approved routing number administrator and supported by the PSAP equipment. (NPD = Numbering Plan Digit; NPA = Numbering Plan Area) If a pANI of the form NPD/NPA-511-XXXX is sent in the MF sequence corresponding to the call back number, the same digit string shall be generated by the LPG and delivered to the legacy PSAP as a pANI that represents location information received by the LPG in incoming signaling.

4.3.4.3 The INVITE message sent by the NIF component to the PIF component shall contain the following information:

- Request Uniform Resource Identifier (URI) = PSAP URI resolving at the gateway
- Max Forwards <70
- Record Route = ESRP URI
- Route header = urn:service:sos
- From To = sip:911@vsp.com

- PAI Via = an identifier for the LPG
- Contact = as received by the NIF component
- Supported = as received by the NIF component
- SDP = as received by the NIF component
- Geolocation = as received by the NIF component
- Call Info = as received by the NIF component
- History-Info = as received (if present in the INVITE message received by the NIF component)
- Reason = as received (if present in the INVITE message received by the NIF component)
- Contact header that contains the trunk group parameters that identify the outgoing trunk group to the destination PSAP, as defined in RFC 4904

4.3.4.4 The NIF shall be capable of initiating to the NG-911 Routing Service the following:

- Call Transfers
- Conferencing

4.3.5 PSAP Interface: LPG (Protocol Interworking Function [PIF] Subcomponent)

The PIF component of the LPG will be responsible for interworking the SIP signaling received from the NIF component with the traditional CAMA MF or E-MF signaling sent over the interface to the destination PSAP.

4.3.5.1 The PIF shall accept SIP INVITE messages generated by the NIF component.

4.3.5.2 Upon receiving the INVITE method, the PIF shall identify the destination PSAP based on the information in the Request URI and select an outgoing trunk to that PSAP based on the outgoing trunk group information in the Contact header.

4.3.5.3 Based on the information received in incoming signaling from the NIF component, the PIF shall generate either traditional MF or E-MF call signaling based on the capabilities of the PSAP telephone equipment.

4.3.5.4 The PIF will also be responsible for accepting hook flash and DTMF signaling (e.g., associated with transfer requests) from the legacy PSAP and sending it to the NIF component in RTP packets, per RFC 2833.

4.3.6 PSAP Interface: LPG (Location Interworking Functions [LIF] Subcomponent)

The LPG must support an ALI interface that can accept an ALI query from the legacy PSAP and return location information based on the formats specified in NENA 04-001 (*Recommended Generic Standards for E9-1-1 PSAP Equipment*) and NENA 04-005 (*ALI Query Service*). Additional information beyond just call back number and location information may be included in an ALI response. There are various ways that ALI data may be obtained by the LPG so that it can be returned to the legacy PSAP in the expected format.

4.3.6.1 If the LPG receives call back information (i.e., in the form of a 10-digit NANP number) and location-by-value in the incoming INVITE message from the ESRP, the LPG shall use this information to populate the call back number and location fields of the ALI response.

4.3.6.2 The LPG shall also generate a CoS for the call.

4.3.6.3 If location-by-reference is received in the incoming INVITE message from the ESRP, the LPG shall query other elements (i.e., location information servers [LISs], LNGs) using an appropriate dereferencing protocol.

4.3.6.4 The LPG shall access "Additional Data" structures to populate other fields in the ALI response.

4.3.6.5 The LPG shall utilize the Hyper Text Transfer Protocol (HTTP) GET method described in IETF RFC 2616.

4.3.6.6 The LPG shall utilize the information contained in the Call Info header of the received INVITE to identify the address of the target subscriber database to which GET will be directed.

4.3.6.7 The LPG shall receive and process the eXtensible Markup Language (XML)-formatted data in the response from the subscriber data, and use it to populate the appropriate fields of the ALI response message.

4.3.7 PSAP Interface: Request for Assistance User Agent (RFAUA)

For incoming SIP and RTP emergency calls, the RFAUA is the SIP element acting on behalf of an identifiable call taker at their answering position. Specific information regarding RFAI and the use of RFAUA is found in the proprietary document from ATIS, *Request for Assistance Interface (RFAI) Specifications*.

4.3.7.1 RFAUA shall initiate and terminate SIP transactions on requests for assistance (RFAs) delivered to the call taker at their answering position.

4.3.7.2 The PSAP receives the location in the SIP INVITE message and shall format an ALI query in order to obtain location information.

4.3.7.3 The RFAUA interface in the NG-911 Routing Service shall provide the following:

- ALI
- IP selective routing functionality
- RFAUA functionality
- Registrar functional entity

4.3.7.4 The proposed NG-911 Routing Service shall provide functionality in accordance with ATIS-0500019.2010 for the following:

- Configurations and state management
- Request notification delivery
- Test calls
- Voice bridging
- RFAUA registration requirements
- RFAI version
- SIP message body extensions
- SIP profiles

In addition to the requirements listed above, Respondents should highlight any distinguishing aspects of their service to be considered during the evaluation for the NG-911 Routing Service.

The remainder of this page is left blank.

4.4 Sub-state ESInet Interconnection Requirements

The following requirements are for the interconnection of sub-state ESInets or NG-911 systems. These sub-state systems are assumed to have emergency call routing capabilities, which distinguishes them from the type of interconnections described in 4.3.

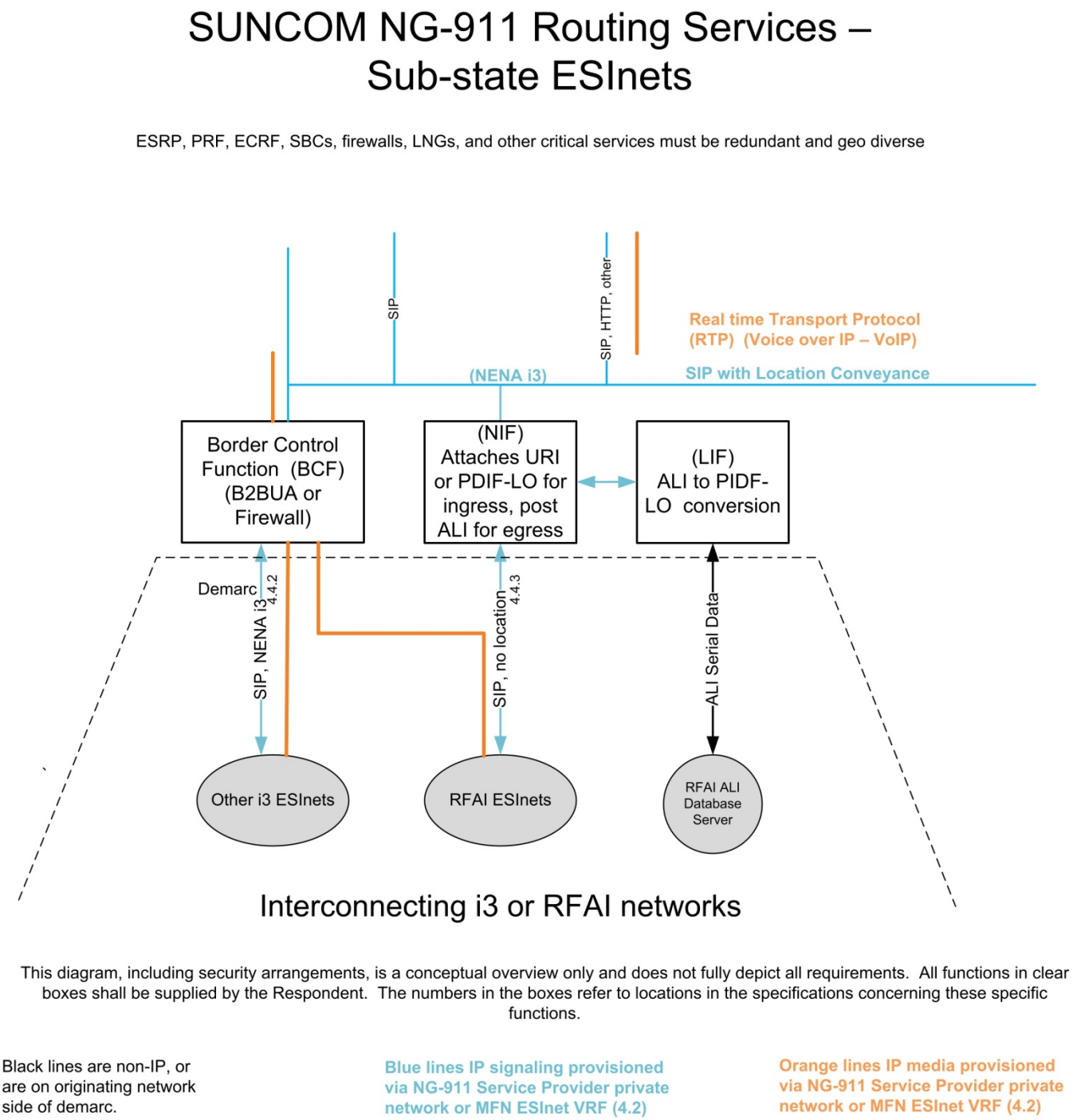


Figure 23—Sub-state ESInet Interconnections

Return to Index

4.4.1 General ESInet Interface Requirements

4.4.1.1 The proposed solution shall interconnect to existing, as defined in section 4.0, and other future ESInets. These will include sub-state ESInets, other states, or governmental ESInets, such as military bases.

4.4.1.2 The successful Respondent shall coordinate with the existing sub-state ESInet providers to interconnect, if requested.

4.4.1.3 Data and calls will be regularly sent back and forth between the NG-911 Routing Service and sub-state systems. Interfaces to other ESInets must support bi-directional emergency call and data delivery. Respondents shall describe the methods used to accomplish this.

4.4.1.4 The successful Respondent shall provide high-level security between the NG-911 Routing Service and sub-state ESInets. This should be accomplished by the use of security zones as described in section 4.7. Respondents shall describe the systems and processes used by the proposed NG-911 Routing Service between sub-state ESInets and the NG-911 Routing Service to provide this communication safely.

4.4.1.5 Transactions shall be recorded in the consolidated transaction log as defined in section 4.6.9.

4.4.1.6 The interface is expected to support information sharing, access control, and other public safety applications and services, such as GIS updates in some instances, in addition to call delivery. Respondents shall describe how their solution facilitates/handles this shared connectivity.

4.4.1.7 Two types of interconnections to sub-state ESInets are expected:

- A sub-state ESInet that has been deployed with the call origination providers sending calls directly to the sub-state ESInet for initial call routing and using the NG-911 Routing Service only for transfers.
- A sub-state ESInet that has been deployed with the call origination providers sending calls to the NG-911 Routing Service for initial call routing and then the NG-911 Routing Service delivers the call to the sub-state ESInet.

These two configurations will have very different bandwidth requirements. Respondents shall describe the interconnection bandwidth required for each type of sub-state ESInet. Respondents shall provide a table, such as in Table 5 below, to illustrate the required bandwidth of their proposed NG-911 Routing Service. It is anticipated that the minimum bandwidth to a sub-state ESInet shall be at least 1.5 Mbps, but Respondents shall describe smaller bandwidths and any economic feasibility to the Department to use them.

Table 5—Sample Bandwidth Table

Typical Bandwidth Size	Sub-State Call Origination Number of Positions, and Calls	State System Call Origination Number of Positions, and Calls
DS-1	Up to XX Positions, and XX Calls	Up to XX Positions, and XX Calls
DS-3	Up to XX Positions, and XX Calls	Up to XX Positions, and XX Calls
10 Mbps	Up to XX Positions, and XX Calls	Up to XX Positions, and XX Calls

4.4.2 Interface Type: NENA i3 Interface

4.4.2.1 Data and calls will be regularly sent back and forth between the NG-911 Routing Service and sub-state systems. Respondents shall describe in detail, including drawings and call flow diagrams, the proposed system's capability to provide and maintain direct bi-directional interconnection to sub-state ESInet and NG-911 systems using the NENA i3 interface.

4.4.2.2 The NG-911 Routing Service shall have DNS implemented, but may use MyFloridaNet systems as a backup if needed. The successful Respondent shall work cooperatively with MyFloridaNet to coordinate, document, and publish public and private DNS identifiers.

4.4.2.3 The NG-911 Routing Service will be interconnected to multiple networks and have a potential for IP address conflicts. Respondents shall describe in detail how IPv4 address conflicts between MyFloridaNet, the NG-911 Routing Service, sub-state ESInets, and other external systems will be resolved.

4.4.2.4 The NG-911 Routing Service shall present and receive calls to and from the sub-state ESInets using the SIP interface requirements as defined in section 4.3.3.

4.4.2.5 All calls shall contain a SIP Location Conveyance Geolocation header commonly referred to as PIDF-LO, as defined in section 4.3.3.

4.4.2.6 Respondents shall describe how they will obtain and maintain high availability and how they will monitor the health of the critical NG-911 Routing Service components or functions on the path between the call origination network and the PSAP, such as the LNG functions and sub-functions, the ESRP and ECRF, and critical SBCs.

4.4.3 Interface Type: RFAI Functions

4.4.3.1 Respondents shall describe in detail, including drawings and call flow diagrams, the system's capability to provide and maintain direct bi-directional interconnection between the NG-911 Routing Service and sub-state NG-911 systems using the RFAI interface.

4.4.3.2 The successful Respondent shall deliver, route, transfer, and bridge emergency calls to sub-state ESInets utilizing RFAI.

4.4.3.3 For 911 calls proceeding from an RFAI system towards the NG-911 Routing Service, the successful Respondent shall provide a gateway that can perform legacy ALI dips and convert the response into NENA i3 formats, either PDIF-LO or URI to the location data or both.

4.4.3.4 For 911 calls proceeding from the NG-911 Routing Service to an RFAI system, the successful Respondent shall provide a gateway that can post the location data in a suitable legacy ALI format (such as E2 or NENA serial data) and present a pANI query key in the RFAI message (in the P.Asserted.Identity [PAI] SIP header) such that the RFAI system can process the call with ALI information. The NG-911 Routing Service must support wireless carrier rebids from the RFAI network.

4.4.3.5 The functions required by 4.3.3 and 4.3.4 may be shared with other LNG components (such as wireline and wireless LNGs) or may be deployed separately, at the Respondent's option. However, Respondents shall fully disclose the details of the proposed NG-911 Routing Service so the Department can determine how Respondents have resolved this issue.

4.4.3.6 If a 911 call originates from a wireless carrier network via legacy trunks and ALI systems, the successful Respondent has the option of passing the original pANI/Emergency Services Routing Key (ESRK) through the state NENA i3 ESInet using private SIP headers or other means to forward the pANI to the RFAI network. However, this approach must not create any issues with other NENA i3 components, including i3-compliant PSAPs that might handle the call as a primary PSAP and then transfer the 911 call to the RFAI network.

4.4.3.7 Regardless, Respondents shall describe the proposed mechanism for resolving state NENA i3 to RFAI interconnection in sufficient detail that the Department can understand exactly how the proposed mechanism will operate and be deployed.

In addition to the requirements listed above, Respondents should highlight any distinguishing aspects of their service to be considered during the evaluation for the NG-911 Routing Service.

The remainder of this page is left blank.

4.5 Call Origination Provider Interconnection Requirements

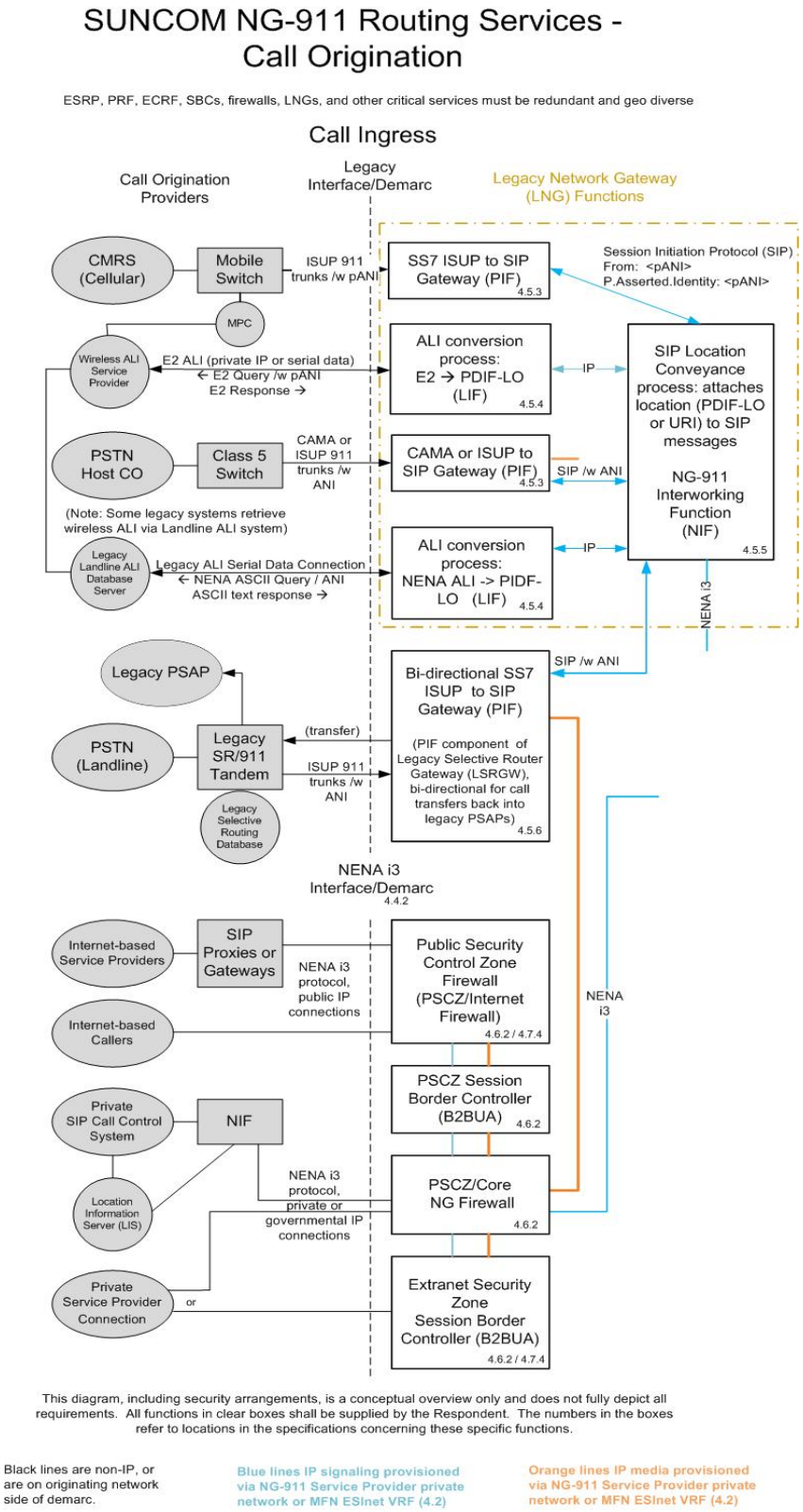


Figure 24—Call Origination Interconnections

Return to Index

4.5.1 General Call Origination Interconnection Requirements

4.5.1.1 The NG-911 Routing Service shall interface with the following systems at a minimum:

- Legacy wireline 911 providers (large and small providers regardless of the providers' capabilities, e.g., CAMA, PSTN, Signaling System 7 [SS7], etc.)
- Commercial Mobile Radio Service (CMRS) cellular providers
- Internet-based providers
- Hosted VoIP providers
- Governmental SIP call control systems (such as large private VoIP systems for federal, state or large local governmental agencies authorized by the State)

4.5.1.2 The NG-911 Routing Service shall accept 911 calls with CAMA services in both analog and digital formats.

4.5.1.3 The NG-911 Routing Service shall accept 911 calls with SS7 services.

4.5.1.4 The NG-911 Routing Service shall accept Integrated Services Digital Network (ISDN) calls with Digital Signal, level 0 (DS0) or DS1 services.

4.5.1.5 Respondents shall provide a clear description of the proposed LNG, list its features and capabilities, discuss its error handling and default mechanisms, and provide an overview of how it is deployed and how high availability of LNG call handling will be achieved.

4.5.1.6 The description of the LNG shall include a discussion of any gaps that the Respondent sees in the existing standard(s) with respect to the conveyance of legacy ALI data, and how the Respondent will work around such issues until they have been resolved in SDOs.

4.5.1.7 Respondents shall provide more than two geographically diverse locations for the termination of call origination circuits to the NG-911 Routing Service. At least one location shall be within the state of Florida. Respondents shall include these locations in their response.

4.5.1.8 Respondents shall provide an LNG that performs the functions of PIF, LIF, and NIF.

4.5.2 NENA i3 Interconnection Requirements

4.5.2.1 All SIP UAs and SIP Proxies supplied by the successful Respondent shall comply with the requirements of IETF RFC 3261. All SIP UAs and SIP Proxies shall also comply with the requirements of any documents that are referenced by RFC 3261, where those additional documents apply to the proposed solution. Respondents shall provide descriptions, drawings, and call flow diagrams to explain how the proposed solution will accomplish this.

4.5.2.2 The interconnection to the call origination providers will be secured as described in section 4.7.4.

4.5.2.3 All SIP components that participate in the SIP signaling for the delivery of emergency calls, as explicitly labeled on the Florida NG-911 Logical Diagram as "NENA i3," shall comply with the requirements of NENA document 08-003. These components shall also comply with the requirements of any documents that are referenced by NENA 08-003, where those additional documents apply to the

proposed solution. Respondents shall provide descriptions, drawings, and call flow diagrams to explain how the proposed solution will accomplish this.

4.5.2.4 It is important for Respondents to understand it is also a requirement to interconnect with IP-based sub-state emergency call networks and PSAPs that conform to ATIS RFAI as specified in document ATIS-0500019. The NENA i3 specification does not necessarily provide means to transport all information required by RFAI through an i3 network. Respondents shall describe how the proposed NG-911 Routing Service satisfies the RFAI interoperability requirement on calls for service received from call origination providers. Respondents shall fully explain their proposed solution via narrative and diagrams.

4.5.2.5 Respondents shall support the NENA i3 interface as defined in section 4.4.2.

4.5.2.6 Origination networks shall present 911 calls to the NG-911 Routing Service meeting the SIP interface requirements.

4.5.2.7 All 911 calls shall contain a Geolocation header.

4.5.2.8 Origination networks that are also access networks should provide a LIS function (location dereference, and location validation if applicable). Respondents shall provide functionality to interface with the provider's LIS or to provide the LIS services if not provided by the call origination provider.

4.5.3 LNG Protocol Interworking Function (PIF)

4.5.3.1 The LNG PIF shall perform the functions listed in section 4.3.5 for 911 calls received from the call origination providers.

4.5.3.2 The LNG PIF shall be sized in a manner that will allow for at least 50 percent more traffic than the average busy hour.

4.5.3.3 The LNG PIF shall determine whether the 911 call is a non-wireless or wireless emergency call based on the incoming trunk group and/or the incoming signaling.

4.5.3.4 The PIF shall support calls received over an MF trunk interface:

- Shall recognize a trunk seizure and return a wink back to the non-wireless switch or mobile switching center (MSC)
- Shall receive and process the appropriate ANI sequence
- If CAMA-type signaling is used, the PIF component shall be capable of receiving and processing an ANI sequence that consists of I + 7-digit ANI
- If Feature Group D operator-type signaling is used, the PIF component shall be capable of receiving and processing an ANI sequence consisting of I + 7-/10-digit ANI
- Shall receive and process Feature Group D signaling that originates in a wireless network
- Shall receive and process an on-hook indication from a non-wireless switch or MSC

4.5.3.5 The PIF shall support calls received over an SS7 Interface:

- SS7 Message Transfer Part (MTP) signaling for 911 call setup

- SS7 ISDN User Part (ISUP) signaling for 911 call setup
- It is assumed that the trunk group from the LEC end office or MSC to the LNG is a dedicated trunk group per carrier

4.5.3.6 If the incoming trunk to the LNG is an SS7-controlled dedicated trunk selected by a wireline end office or wireless MSC, the PIF component of the LNG shall receive and process an ISUP Initial Address Message (IAM) containing parameters populated as described in GR-2956-CORE, *CCS/SS7 Generic Requirements in Support of E911 Service*, Sections 5.2.1.2.1, R2956-77 and 5.2.1.4.1, R2956-82, respectively.

4.5.3.7 The PIF shall receive and process an ISUP Release (REL) message from a wireline end office or MSC, formatted as described in Table A-5 of GR-317-CORE, and generating a Release Complete Message (RLC) formatted as described in Table A-6 of GR-317-CORE in response.

4.5.3.8 The PIF shall receive and process supervisory ISUP messages sent by LEC end offices and MSCs (e.g., Blocking, Blocking Acknowledgement). The PIF component shall follow the procedures described in Section 3.1.4 of GR-317-CORE for processing these messages.

4.5.3.9 The PIF shall support receipt of both ANI and pANI.

4.5.4 LNG Location Interworking Functions (LIF)

4.5.4.1 The LNG LIF shall perform the functions listed in section 4.3.6 for calls received from the call origination providers.

4.5.4.2 The LNG LIF shall be sized in a manner that will allow for at least 50 percent more traffic than the average busy hour.

4.5.4.3 The LIF queries legacy ALI database(s) using the ANI or pANI that is delivered via the CAMA or ISUP trunk signaling.

4.5.4.4 The database system must also be capable of steering pANI/ESRK queries to wireless ALI service providers (WASPs) using the E2 ALI query format. (E2 is described in NENA document 05-001.) The successful Respondent shall be responsible for working with WASPs to establish appropriate wireless ALI connections.

4.5.4.5 The LIF shall communicate with other LNG sub-functions and NG-911 services via IP, using the NG-911 Routing Service as needed.

4.5.4.6 The LIF ALI system shall support a location query via the HELD protocol for wireless location data and wireless rebids, and provide a mechanism for any limitations on the rebid capabilities of the call origination providers.

4.5.4.7 The LNG shall support a default routing capability in the event a timely response is not received from the ALI database. This default routing may be accomplished by providing default locations, but other

solutions are acceptable provided they are compatible with other NG-911 services. All default locations shall be coordinated with the Department and Counties.

4.5.5 LNG NG-911-specific Interwork Function (NIF)

4.5.5.1 The LNG NIF shall perform the functions listed in section 4.3.4 for calls received from the call origination providers.

4.5.5.2 The LNG NIF shall be sized in a manner that will allow for at least 50 percent more traffic than the average busy hour.

4.5.5.3 The NIF shall use standard interworking procedures, as defined in ATIS T1.679-2004, IETF Internet Draft draft-patel-dispatch-cpc-oli-parameter-02, and IETF Internet Draft draft-york-sipping-p-charge-info-08, to generate a SIP INVITE message based on incoming MF or SS7 signaling, and pass that INVITE message to the NIF component of the LNG.

4.5.6 Bi-directional Protocol Interworking Function (PIF)

4.5.6.1 Respondents shall provide the functions at the call origination providers' interface, at a minimum, for bi-directional signaling on the in-use trunks.

4.5.6.2 Signaling shall support all provisioned 911 signaling or functionality on the legacy providers' networks, and at a minimum the following:

- Hook Flash
- Short code signals, such as Star code
- DTMF
- On/off hook

In addition to the requirements listed above, Respondents should highlight any distinguishing aspects of their service to be considered during the evaluation for the NG-911 Routing Service.

The remainder of this page is left blank.

4.6 Core NG-911 Function Requirements

This section specifies functions that support emergency call routing, call control, call forwarding, and call delivery within the Florida NG-911 Routing Service. All call signaling processed by the NG-911 Routing Service utilizes SIP in NENA i3-compatible formats, complete with SIP location conveyance. A generic overview of the NENA i3 Functional Elements in the context of an ESInet is depicted in Figure 25. The components inside the blue cloud are interconnected using IP networking technology.

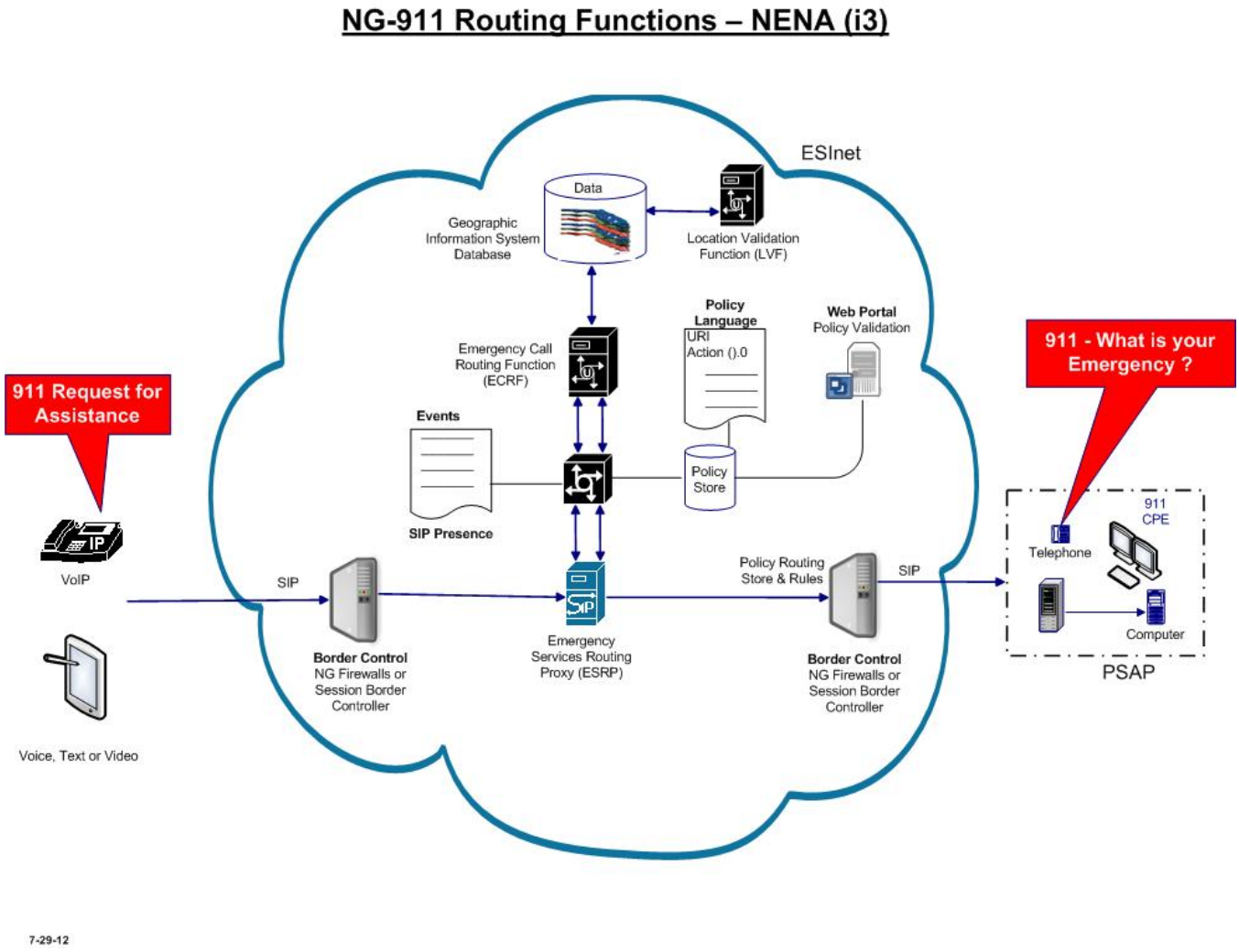
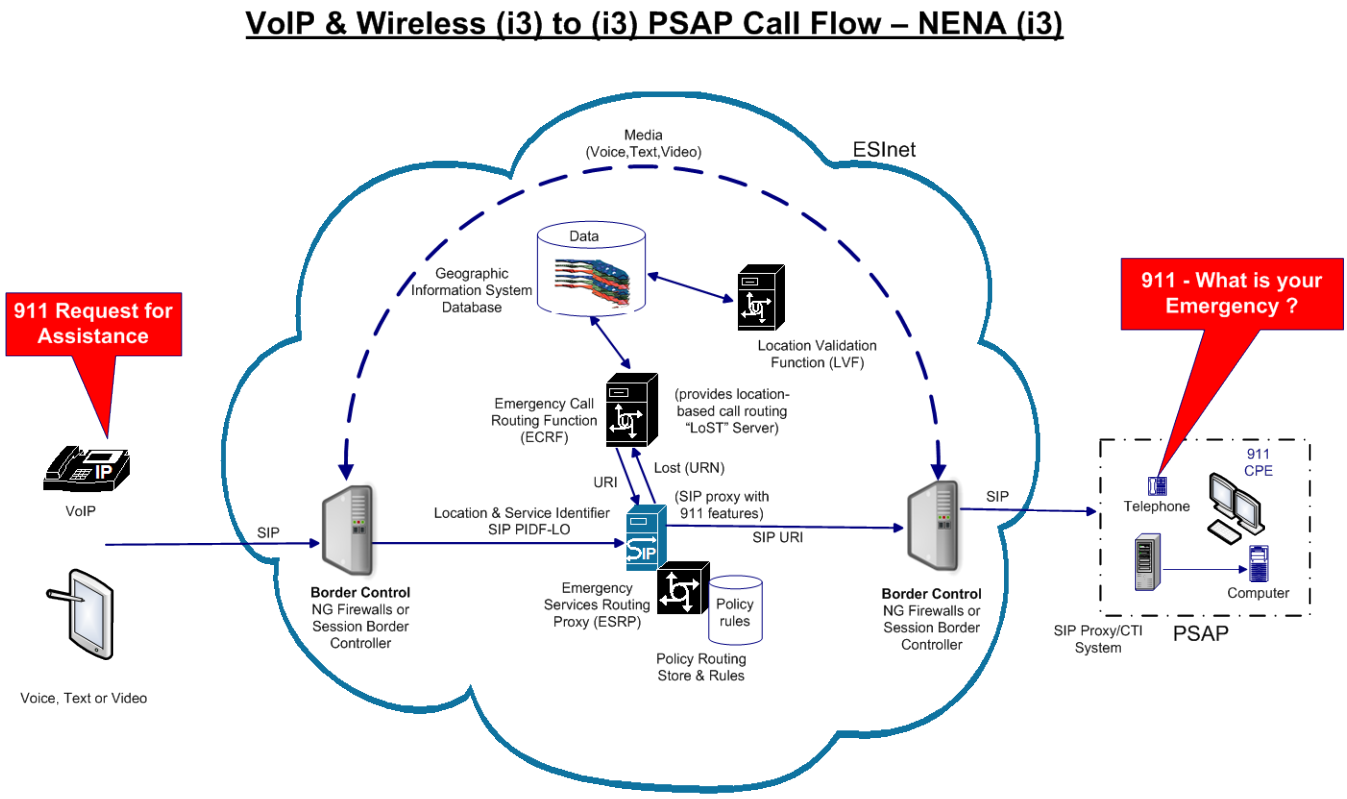


Figure 25—ESInet Functional Elements

Emergency calls originate from sources within or connected to the NG-911 Routing Service, and are forwarded or delivered to PSAPs, to a sub-state ESInet, to legacy 911 tandems, or to an ESInet in another state or federal agency. Figure 26 is a conceptual representation of emergency calls flowing from wireless carriers or VoIP telephone systems to a modern NENA i3 PSAP using native i3 protocols.



PIDF-LO contains location Presence Information Data Format Location Object – location information attached to a SIP message
Location to Service Translation (LoST) Protocol Queries with location information and a Service URN and returns a URI
Universal Resource Name intended to serve as persistent, location-independent resource name
Uniform Resource Identifier (URI) used to identify a resource on a network

Figure 26—VoIP and Wireless Call Flow

The remainder of this page is left blank.

Return to Index

Figure 27 depicts emergency calls being forwarded to another sub-state ESInet, rather than directly to a PSAP. A key concept in NG-911 is the idea of easily interconnected networks.

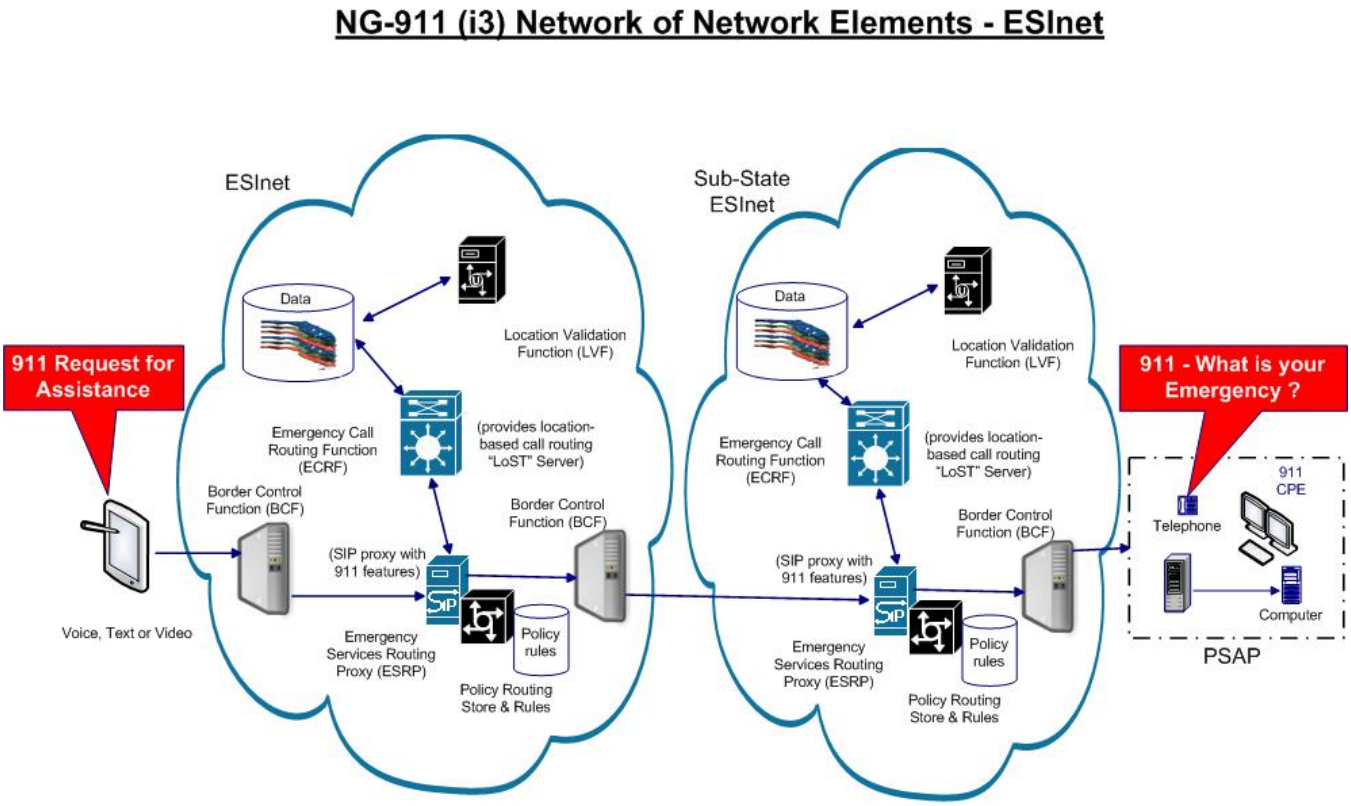


Figure 27—Emergency Call Forwarding

The remainder of this page is left blank.

Gateway functions are required to interconnect to legacy 911 systems and/or systems utilizing other (non-NENA i3) signaling and non-IP transport formats. Figure 28 depicts calls originating from a legacy wireline telephone system being transported across the NG-911 network and (in this case) being delivered to a legacy 911 PSAP. This illustrates a key concept in the design of the Florida NG-911 Routing Service – all ingress traffic is converted to NENA i3 protocols for processing in the NG-911 Routing Service, and then converted back to other protocols at the egress point if the downstream system or PSAP does not yet support NENA i3 protocols.

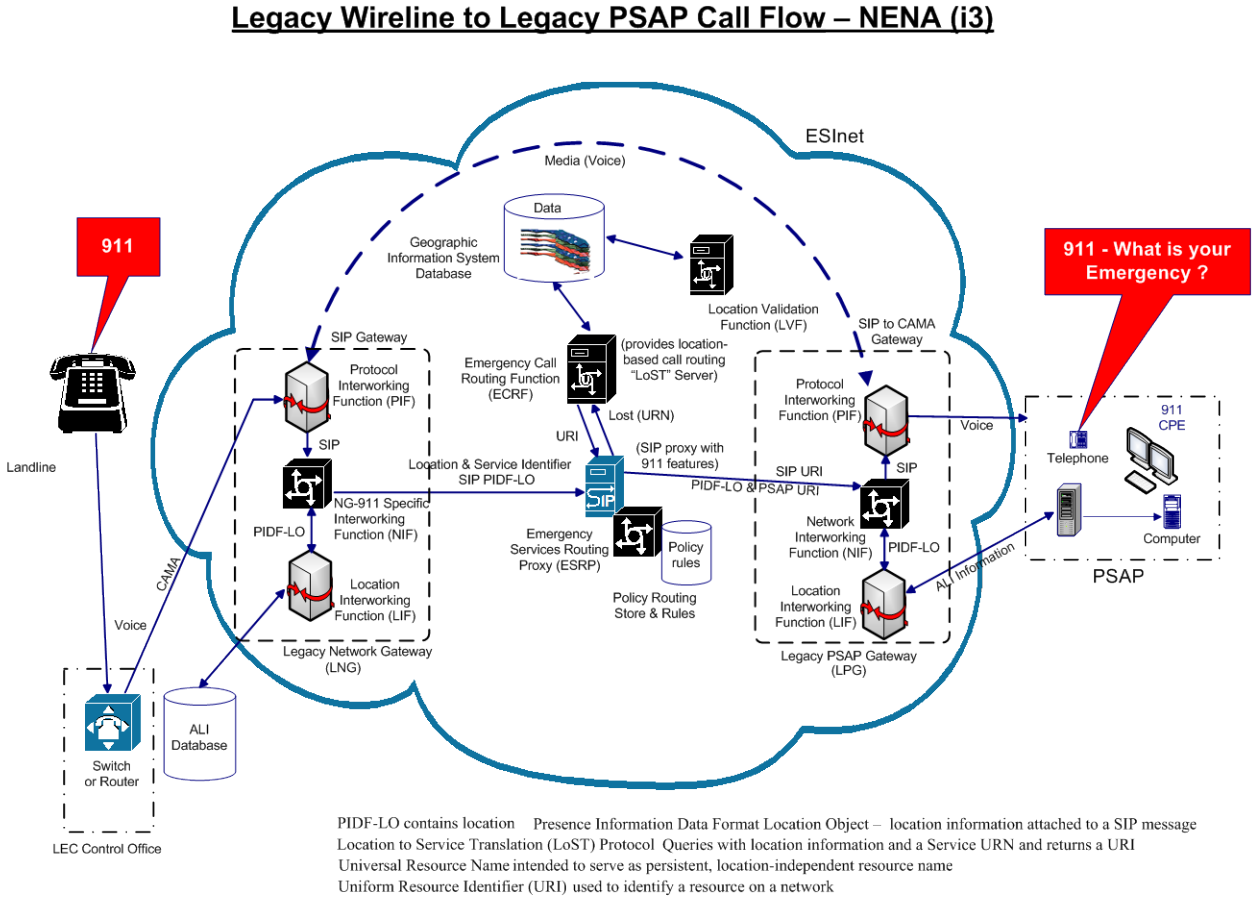


Figure 28—Legacy Wireline to Legacy PSAP Call Flow

Figure 29 depicts some intermediate level of detail and, more precisely, the functions required in the Florida NG-911 Routing Service as specified in the remainder of this section. The clear boxes represent functions to be supplied by the successful Respondent, while the shaded boxes are external to the NG-911 Routing Service. This is a logical diagram because nearly all the required functions must be deployed in multiple instances across geographically diverse sites in order to satisfy the high availability and reliability requirements of the Florida NG-911 Routing Service. An actual deployment diagram of the devices and servers required to implement the NG-911 Routing Service would be much more complex with many more parts.

All SIP signaling and media transport in the core of the Florida NG-911 Routing Service shall utilize IPv6. Monitoring and certain auxiliary functions (e.g., SNMP) may be deployed via IPv4 using dual stack if IPv6 monitoring tools are not available, but only if using IPv4 in this way has no adverse impact on the NG-911

functions and if this use of IPv4 creates no future migration issues with respect to the NG-911 call routing and call delivery functionality. Use of IPv4 is deprecated.

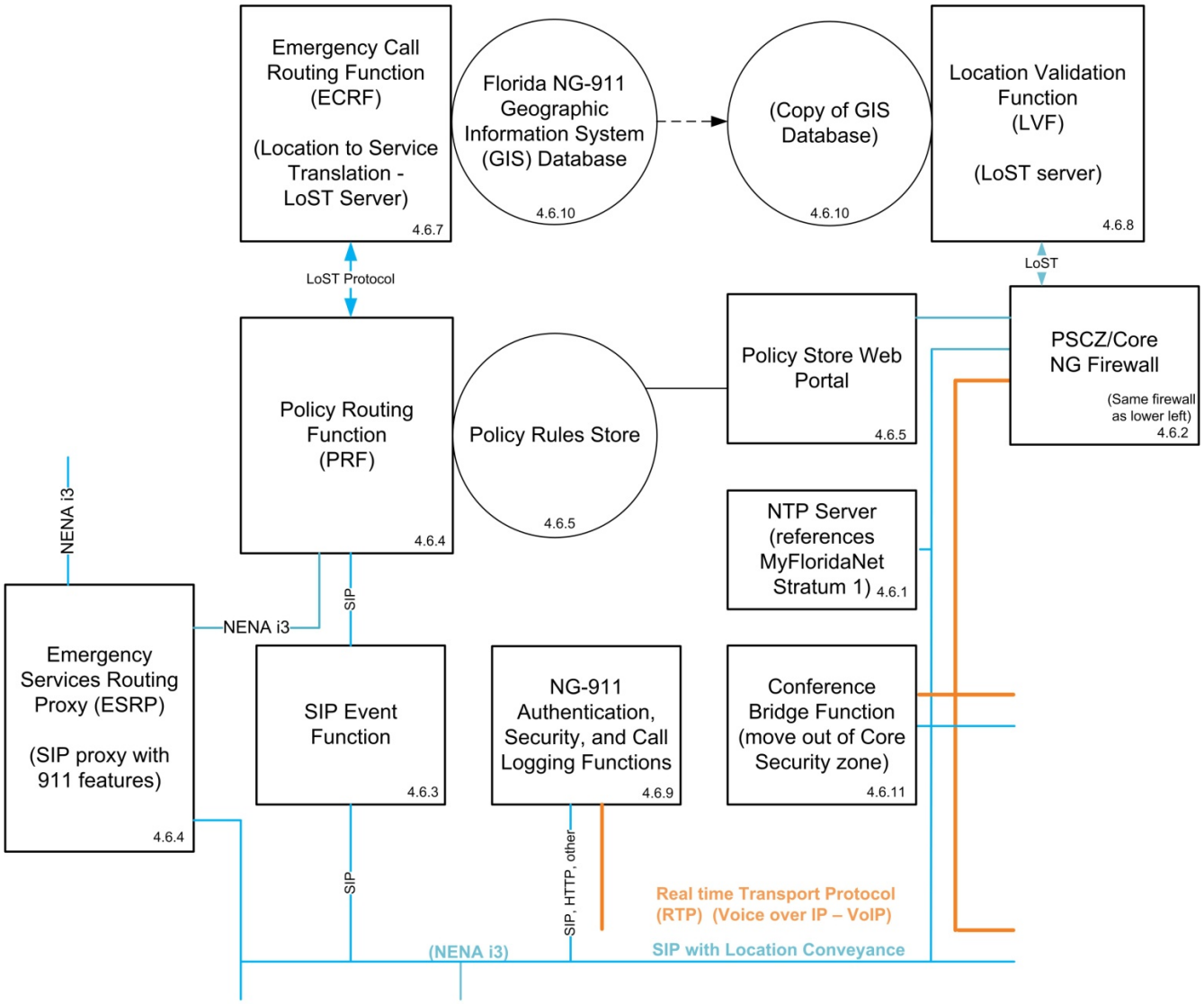
This section also specifies functions supporting destination status (presence), certain call conferencing and transfer schemes, and application-specific security functions.

This section does not prohibit the packaging of the functions or the processes that implement these functions. For example, the Policy Routing Function (PRF) and ESRP may be combined into a single software process or be separate processes running on separate hardware devices. Respondents shall explain via diagrams and narrative how the proposed NG-911 Routing Service implements the required functions and meets NENA i3 standards.

The remainder of this page is left blank.

SUNCOM NG-911 Routing Services – Core Services

ESRP, PRF, ECRF, SBCs, firewalls, LNGs, and other critical services must be redundant and geo diverse



This diagram, including security arrangements, is a conceptual overview only and does not fully depict all requirements. All functions in clear boxes shall be supplied by the Respondent. The numbers in the boxes refer to locations in the specifications concerning these specific functions.

Black lines are non-IP, or are on originating network side of demarc.

Blue lines IP signaling provisioned via NG-911 Service Provider private network or MFN ESInet VRF (4.2)

Orange lines IP media provisioned via NG-911 Service Provider private network or MFN ESInet VRF (4.2)

Figure 29—Core Services

Return to Index

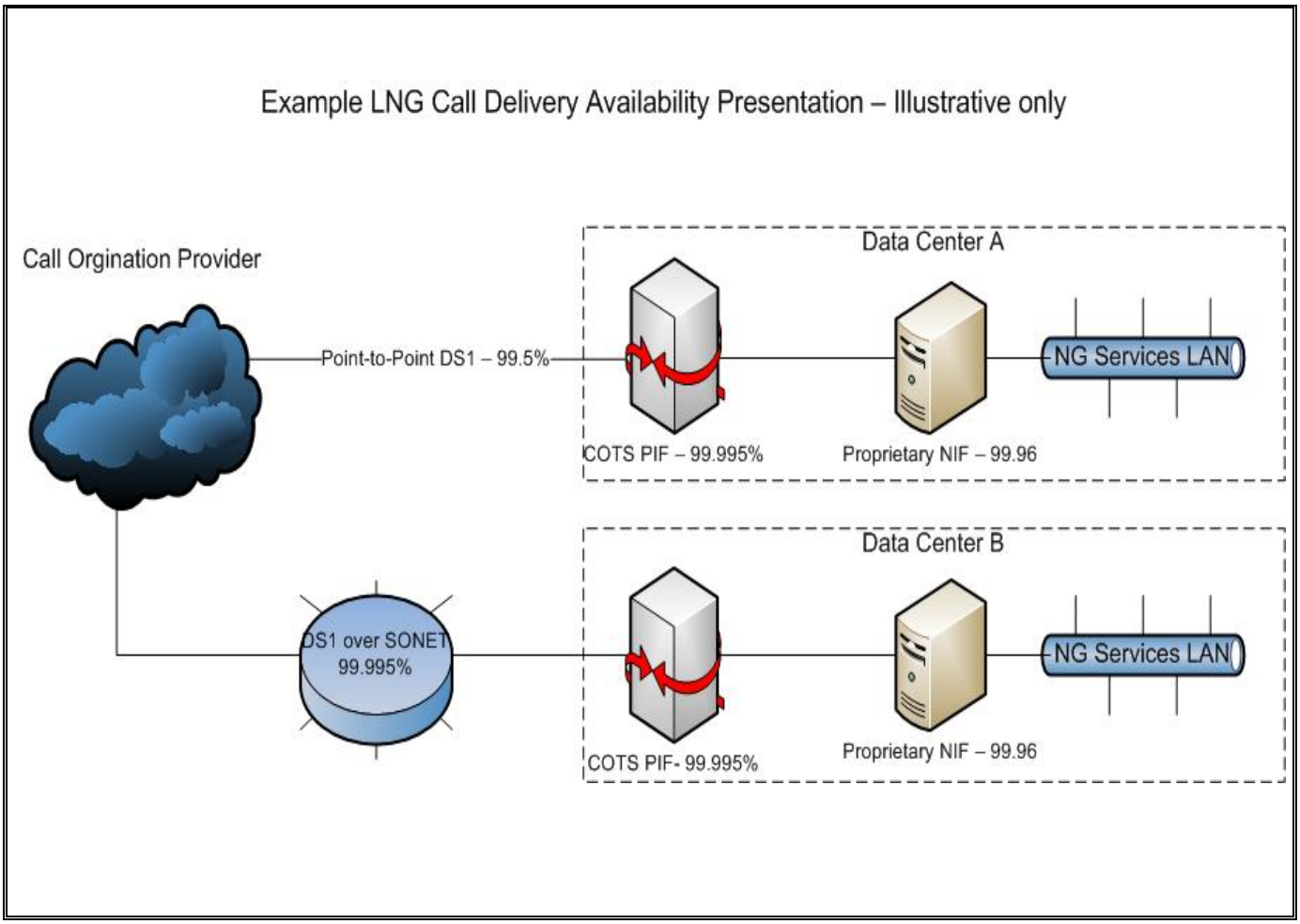
4.6.1 General NG-911 Functions Requirements

4.6.1.1 Respondents shall present convincing evidence, to include diagrams and calculations, to illustrate that the Respondent will be able to satisfy the high availability, high reliability, traffic throughput, and latency requirements for each critical function as identified and specified throughout this section. Simply stating that the proposed system or critical function can satisfy these requirements will be judged non-responsive.

Respondents shall state the basis for reliability, availability, traffic flow, and processing delay/latency data for each component used in providing a critical function. This data shall be displayed on a diagram showing the serial/parallel relationships of the components. Respondents shall display the calculations used to compute the reliability, availability, throughput, and processing delay/latency of each critical function, accompanied with a narrative explaining the analysis.

Table 6 illustrates an acceptable response, including a diagram, table, and narrative display. This example concerns the availability of an LNG, and is illustrative only. Respondents shall document their availability values and justify their assumptions.

Table 6—Example Acceptable Response



Return to Index

The availability calculations for this example follow:

Component	Availability	Basis	Overall Availability
Point-to-Point DS1	99.5%	Service Provider SLA	
COTS PIF	99.995%	Calculated from manufacturer claimed 200,000 MTBF and Respondent's 4 hour repair time	
Proprietary NIF	99.96%	Calculated from 4 hours downtime / year (allowance for software update & maintenance)	
LNG at Data center A		= 0.995 * 0.99995 * 0.9996 (series formula)	99.4%
DS1 via SONET	99.995%	Service Provider SLA	
LNG at Data center B		=0.99995 * 0.99995 * 0.9996	99.95%
Overall LNG		=1-((1-0.994)*(1-0.9995)) (parallel formula)	99.9997%

The discussion for this example follows:

The above example demonstrates that the LNG solution obtains five nines availability.

There are two diverse paths from the call origination provider network to diverse Florida NG-911 Routing Service data centers. An availability value is assigned to each component on each path.

For the circuits, the availability is based upon the service provider's SLAs for the circuit as provisioned.

For the gateways (PIFs), which are commercial off-the-shelf (COTS) products, the manufacturer specifies a 200,000 hour mean time between failures (MTBF). Since spare gateways are stocked at the data center, the worst-case time to repair is credibly assigned as four hours. These four hours are the time required to replace a gateway, including the time required to get a technician on-site and to configure the replacement gateway. So the availability of the gateway is calculated as = MTBF /(MTBF + repair time).

The proprietary NIF process (software) runs on a COTS server with a MTBF of 150,000 hours under a Linux OS. Four hours are allowed for downtime for software updates and server reboots, per year. Since there are 8,760 hours in a year, the NIF availability = 8760/8764, or 99.96 percent. Since this is substantially lower availability than might be expected from hardware failures alone (see the PIF discussion above), hardware failures will have little additional impact on NIF availability in this example and has been ignored.

The overall reliability of each of the paths from the call origination provider to the Florida NG-911 Routing Service is the product of the availabilities of all the components on each path, since these devices are in series, and a failure of any one of them fails the path. The two paths, however, are in parallel, and either path can deliver emergency calls if the other path is not operational. The parallel formula shown in the table computes the overall availability of the system, given the availability of each path.

4.6.1.2 The NG-911 Routing Service shall be able to deliver emergency calls to human call takers 99.999 percent of the time during conditions that generate up to three times the average Florida daily emergency call volume, assuming idle call takers are available somewhere within the system. The NG-911 Routing Service shall forward an emergency call towards the most preferred destination under the circumstances at the time of the call, as defined by the then active policy rule-sets and location databases. The overall availability, reliability, and throughput of the system shall be documented in accordance with section 4.6.1.1, using the critical functions specified in this section as the components of the overall NG-911 Routing Service.

4.6.1.3 When in an "all up" status, the Core NG-911 Routing Service functions shall be able to accommodate a sustained traffic flow of at least three times the average Florida daily emergency call volume, and a busy hour of up to six times the average daily busy hour call volume, or at least 8,100 calls per hour, whichever is greater, without encountering performance, memory, bandwidth, or other call delivery limitations. This response must be documented as illustrated in section 4.6.1.1.

4.6.1.4 The Core NG-911 Routing Service functions shall be deployed in at least three geographically diverse TIA Tier 3 or higher data centers separated from each other by at least 80 miles and separated by at least 200 miles at the furthest extent. At least three data centers meeting the geographic separation requirements shall be physically located within the state of Florida and be in an active-active state load sharing all functions. Respondents shall provide documentation that each data center is certified by TIA-942 or American National Standards Institute (ANSI)/Building Industry Consulting Service International, Inc. (BICSI)-002/2011 to be at least 99.98 percent available.

4.6.1.5 Data center to MyFloridaNet connections are the responsibility of the successful Respondent. Data center to MyFloridaNet connections shall be redundant and geo-diverse, and shall provide for automatic failover of IP connectivity in less than four seconds.

4.6.1.6 In the event of the total destruction of or loss of connectivity to a single data center, the surviving system shall remain fully operational with a capacity of at least 100 percent of requirements in section 4.6.1.3 above. Failover of all critical applications shall be automatic and shall occur in less than 25 seconds.

4.6.1.7 All functions required in this section shall be monitored for health status 24x7x365. Detailed monitoring requirements are specified in section 4.7.2 of this document. Respondents shall discuss the impact to 911 calls, if any, of function instances that are out-of-service.

4.6.1.8 The successful Respondent shall provide a NTP server at each data center, located within the Core NG-911 Routing Service security zone. These NTP servers shall be the "master" clock source for all NG-911 Routing Service functions, and shall synchronize to MyFloridaNet Stratum 1 NTP servers. All NTP service users located outside of the Core NG-911 Routing Service security zone must be served from NTP Stratum 2 servers, which are located in adjacent security zones.

4.6.1.9 All NG-911 Routing Service functions required in this section shall maintain network date and time synchronization utilizing NTP from NTP Stratum 1 or Stratum 2 NTP servers as specified in section 4.6.1.8, and accurate to within 0.01 seconds.

4.6.1.10 All functions required in this section shall maintain operational logs (process start/stop, status changes, etc.) and shall output transactional (call detail) logs for real-time or near real-time input into a system-wide logging system as described in section 4.6.9 below. All log entries shall be date and time stamped to 0.1 seconds accuracy using the synchronized time required by section 4.6.1.9.

4.6.1.11 All functions required in this section shall utilize the SIP protocol and comply with the RFC 3261, and shall support the transport of SIP messages by TCP and by TLS.

4.6.1.12 All functions required in this section shall be individually maintainable on an instance-by-instance level. It is unacceptable to require the take-down of an entire required Core NG-911 Routing Service function to perform a maintenance activity. Software upgrades to any critical component must be hitless to the emergency call traffic levels specified in 4.6.1.3 and be backward compatible at least one version level.

4.6.1.13 The Core NG-911 Routing Service functions shall be scalable to support increased call volume, a larger number of interconnections, or other important growth parameters, without taking down the entire system. Ideally, the NG-911 Routing Service capacity can increase simply by adding additional instances of a particular function to the NG-911 Routing Service.

4.6.1.14 The time interval required to signal a call through the NG-911 Routing Service from ingress demarcation to egress demarcation shall be sufficiently short such that the service does not introduce call processing delay normally noticeable to the human users – either the caller or the call taker. In normal call processing (system in all up status, destination operational, normal traffic flows), the signaling delay shall be less than 600 milliseconds. Worst case call setup times shall not exceed three seconds. CAMA trunk signaling conversion is not charged to this time interval.

4.6.1.15 Voice latency through the NG-911 Routing Service from ingress demarcation to egress demarcation shall not exceed 250 milliseconds when the voice channel is routed through a conference bridge, and shall not exceed 150 milliseconds when the voice channel is a single path from ingress to egress, that is, not in a conference, provided the IP network latency is operating within the Respondent's requirements.

4.6.1.16 Respondents shall explain how the proposed GIS system (section 4.6.10) implementation and processes shall be modified, as required, to support additional Spatial Information Function (SIF) data when and as SIF data becomes available. For example, an Open Geospatial Consortium (OGC)-compliant web feature server might be added to the LVF (section 4.6.8) in such a way as to permit PSAPs and other authorized entities to contribute GIS data to ECRF/LVF layers. However, such a process must be documented and controlled in such a way as to not compromise the location-based 911 call routing functions of the ECRF (section 4.6.7).

4.6.2 Border Control Function (BCF)

The security model discussed in sections 4.1 and 4.7.4 requires BCFs at the boundaries or perimeters of the required security zones. Two general types of BCFs shall be utilized within the NG-911 Routing Service:

- Firewalls
- SBCs

4.6.2.1 Next Generation Firewalls

Firewalls may range from simple IP/port ACL restrictions provided by the interconnecting routers to next generation firewalls as specified in section 4.3.2 to IPS devices. Next generation firewalls are intelligent security appliances that perform deep packet inspection and apply heuristics to identify viral payloads and suspicious activity patterns. IPSs further block transmission of suspect packets. The use of IPS functions in the NG-911 Routing Service must be carefully considered so as not to risk emergency call delivery failure.

Since much of the emergency call activity within the NG-911 Routing Service involves the SIP protocol, SIP-aware firewalls (sometimes referred to as "pinhole" firewalls) observe SIP packets and, on demand, dynamically open and close paths for the RTP packets between devices operating in different security zones as described in section 4.7.4. Note that the use of SIP-aware firewalls prevents the use of SIP packet encryption and prevents the use of NAT or NAT-like devices that might change packet IP addresses in conflict with the IP addresses contained within SIP messages.

4.6.2.1.1 Physically separate next generation firewalls shall be provisioned at the public Internet to PSCZ boundary, and at the PSCZ to the Core NG-911 Routing Service security zone boundary. (See Security Diagram in Exhibit B for an example.)

4.6.2.1.2 The successful Respondent shall be responsible for supplying, provisioning, and maintaining IPS-capable next generation firewalls at each interconnected PSAP, sub-state ESInet interconnection, or IP-based ECON service provider interconnection that does not use or is not interconnected via a B2BUA or an SBC.

4.6.2.1.3 All firewalls shall log suspect activity to the SIM system specified in section 4.7.4.12.

4.6.2.1.4 The reliability and availability of core firewalls shall be considered with respect to the requirements of sections 4.6.1.1 through 4.6.1.3. Data center and redundant ingress/egress interconnections will require redundant firewalls to achieve the required availability. Respondents shall provide a detailed design that clearly identifies the devices in the proposed NG-911 Routing Service that are considered to be in the core and that require redundancy.

4.6.2.2 Session Border Controllers (SBCs)

Connections involving the highest security require the use of B2BUA SBCs. These SBCs are essentially SIP-aware gateways that terminate a SIP call and anchor the media on one interface and then generate a new SIP call and transcode the media on another interface. Due to expense and complication, the use of SBCs should be avoided unless specifically needed to provide the highest level of security or to resolve certain types of problems. SBCs can resolve incompatible IP address space assignments, interconnect IPv4 and IPv6 networks, transcode media between different CODECs, and map incompatible dial plans (SIP user names) between interconnection points. Due to the fact that SBCs anchor media, they can become a problem when future new media types are deployed in the NG-911 Routing Service. They can also create points-of-failure that impact the general high availability requirements, especially section 4.6.1.2. Respondents' detailed designs must clearly identify these devices and the physical and logical locations in the proposed NG-911 Routing Service.

4.6.2.2.1 Any SBCs deployed in the NG-911 Routing Service must properly forward SIP MIME (multi-purpose Internet mail extensions) attachments, such as the PIDF-LO, across the border.

4.6.2.2.2 A dedicated and physically separate B2BUA SBC shall be required to interconnect emergency calls from the public Internet to the NG-911 Routing Service. This SBC shall be located within the PSCZ.

4.6.2.2.3 An SBC is required within the MyFloridaNet demilitarized zone (DMZ) for the purpose of interconnecting sub-state ESInets or ECON provider networks as interconnection arrangements require. This SBC may be shared among several uses, provided proper security zone perimeters are maintained. Additional SBCs may be provisioned as circumstances require.

4.6.2.2.4 All SBCs shall log suspect activity to the SIM system specified in section 4.7.4.12.

4.6.2.2.5 The reliability and availability of core SBCs shall be considered with respect to the requirements of sections 4.6.1.1 through 4.6.1.3. System redundancy is required for the BCFs specified in sections 4.6.2.6 and 4.6.2.7.

4.6.3 SIP Event Function

NG-911 functions, particularly the PRF, utilize status information to determine the most desirable handling of an emergency call under the current circumstances, e.g., conditions of extreme call volume, system problems, PSAP overload or PSAP unavailability. The SIP Event Function may also play a role in keeping PSAP operators apprised of events that might impact local PSAP operations, such as an overload condition at a neighboring PSAP or that all fire responders in a particular service area are currently deployed.

The remainder of this page is left blank.

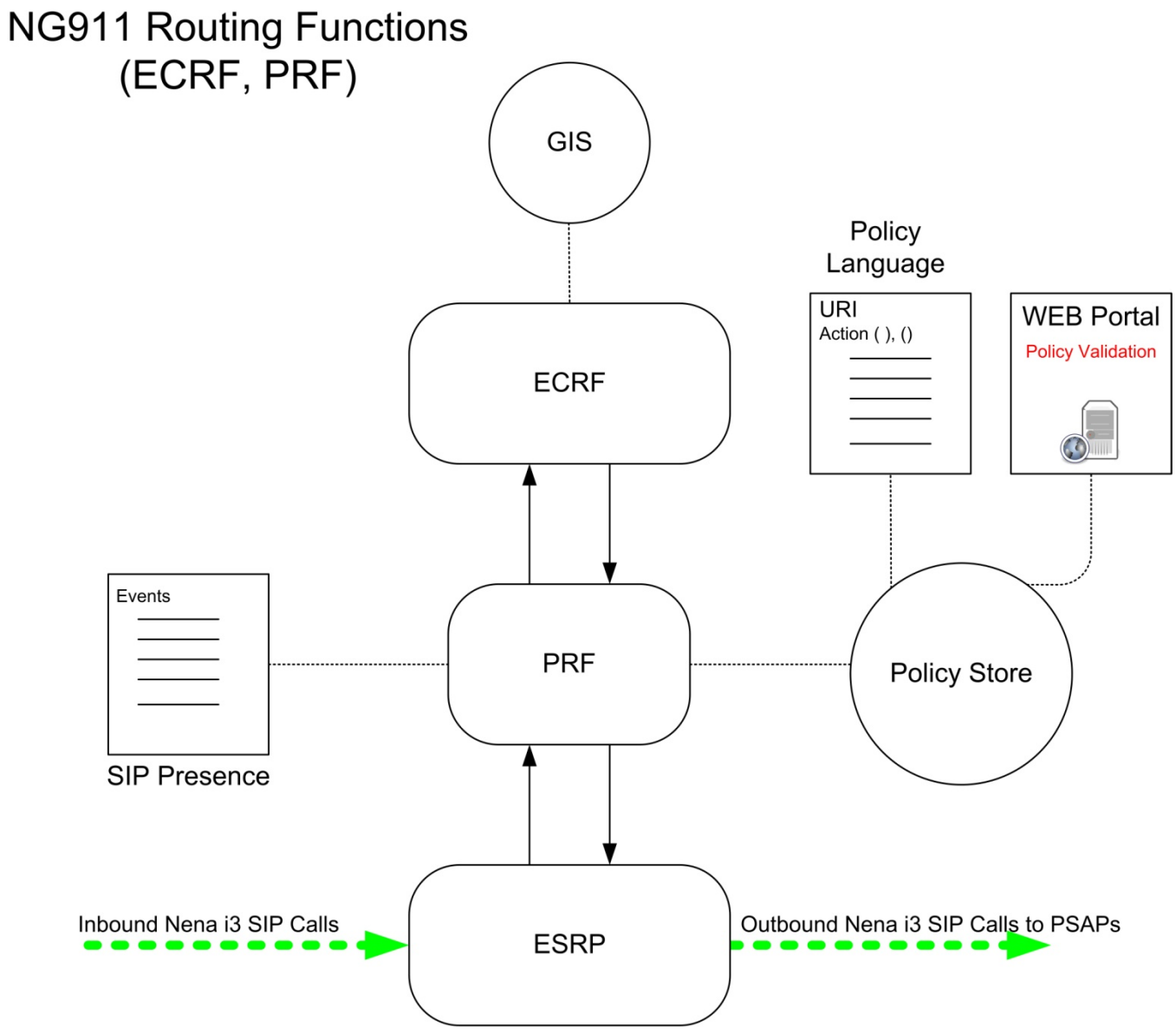


Figure 30—NG-911 Routing Functions

4.6.3.1 Respondents shall supply a SIP Event Function (also known as a SIP Presence service) as a part of the NG-911 Routing Service functions. The SIP Event Function shall implement presence applications, which are called event packages. The data record that records the current status of any particular device, process, or person is called presentity.

4.6.3.2 The SIP Event Function shall implement the SIP SUBSCRIBE, NOTIFY, and PUBLISH methods in compliance with RFC 3265, and shall implement event packages as described in RFC 3856.

4.6.3.3 The SIP Event Function shall specifically implement the NENA event packages as specified in NENA document 08-003, such as nena-SecurityPosture and nena-ElementState. A general purpose SIP-based presence service that can implement additional event packages is highly desirable.

4.6.3.4 The SIP Event Function shall support a necessary and reasonable number of presentity records in accordance with the expected use of the event package. For example, the nena-ElementState event package must support several hundred presentity records, one for each call handling process or call answering instance in the NG-911 Routing Service. This would include the status of each PSAP, each gateway, each SIP proxy, each ECRF instance, and all other major components of the NG-911 Routing Service.

4.6.3.5 The SIP Event Function shall support standard SUBSCRIBE message bodies in accordance with RFC 4661. These are standard XML-formatted messages whereby an event subscriber can describe and filter the events or status changes of which the subscriber requires notification.

4.6.3.6 Respondents shall describe and demonstrate how this function is deployed in the proposed NG-911 Routing Service. Respondents are encouraged to use diagrams to depict the SIP Event Function.

4.6.4 Emergency Services Routing Proxy (ESRP)

The ESRP is a critical function in the delivery of emergency calls via the NG-911 Routing Service. Respondents shall supply a highly available and reliable ESRP function that is 99.999 percent available and reliable.

In these specifications, the actual routing of emergency calls is defined in the PRF. At Respondents' options, the PRF may be packaged as a subcomponent of the ESRP or the PRF may be deployed separately.

The ESRP, or, at a Respondent's option, a separate but integrated SIP proxy function, shall be able to support administrative calls between call takers and PSAP administrators, and to destinations in the PSTN, as required to support situations that often arise in the handling of emergency calls and coordinating responses to emergency situations. Examples of the uses of such administrative functions include adding a doctor or emergency room consultant to an emergency call involving a medical emergency, emergency call takers coordinating their response to an emergency situation, and PSAP administrators dealing with communication system outages in a geographic area.

4.6.4.1 The ESRP shall comply with the general requirements of section 4.6.1 above.

4.6.4.2 The ESRP shall comply with the functional specifications of NENA 08-003 for originating ESRPs.

4.6.4.3 For emergency calls arriving with a SIP Geolocation header containing other than a cid:URI parameter (implying location-by-value), the ESRP shall dereference the URI in an attempt to obtain the call's location data. Alternatively, this process may be a part of the PRF.

4.6.4.4 The ESRP shall implement a HTTP Enabled Location Determination (HELD) interface for dereferencing location-by-reference SIP location messages, or this capability shall be deployed in the PRF.

4.6.4.5 The ESRP shall support TCP for the transport of SIP and HELD messages.

4.6.4.6 The ESRP shall support the invocation of distinct routing policies based on the incoming call queue, incoming URI, or IP address of the call source.

4.6.4.7 The supplied ESRP shall support the registration of SIP telephones at least equal in number to the number of supported emergency call answering telephones. The supplied ESRP shall support seamless calling, conferences, transfers, and other typical private branch exchange (PBX)-like functionality between non-emergency call answering phones, emergency call answering phones, incoming emergency calls, and PSTN trunks accessed via gateways. Emergency call answering positions shall be able to initiate and answer non-emergency PSTN calls, conference and/or transfer emergency calls in progress to PSTN destinations, and call between answering positions. For example, it must be possible to conference in language translation services (reached via an 800 number) onto an emergency (911 dialed) call in progress, or for an answering position to initiate a PSTN call to an automotive towing service provider via the NG-911 Routing Service.

4.6.4.8 Alternatively, Respondents may satisfy section 4.6.4.7 by supplying an additional SIP proxy(s) that provides PBX-like functionality for administrative calling. However, these additional SIP proxies must be able to interoperate with the ESRP/NG-911 Routing Service in such a way that emergency call answering telephones have a seamless experience accessing on-net and PSTN telephones.

4.6.4.9 Respondents shall state the maximum number of calls per second the proposed ESRP solution can sustain for at least one minute under "all up" conditions.

4.6.4.10 Respondents shall describe and list the features of the proposed ESRP, with particular emphasis on how it meets the general requirements of this section (4.6.1 above) and the specific requirements herein. In particular, Respondents shall discuss how high availability is achieved per section 4.6.1.1, and how the ESRP scales.

4.6.5 Policy Routing Function (PRF)

4.6.5.1 The PRF is a critical function in the delivery of emergency calls via the NG-911 Routing Service. Respondents shall supply a PRF that is at least 99.999 percent available and reliable. The PRF may exist as a component of the ESRP implementation, or as a separate component.

4.6.5.2 The PRF shall comply with the functional specifications of NENA 08-003 and the general requirements of section 4.6.1 above.

4.6.5.3 The PRF must support at least the following:

- Alternate routing per PSAP (such as PSAP busy or unreachable)
- Default routes (such as based on incoming gateway trunk ID, call source IP address, ANI exchange code, or similar such available data) – It is highly desirable (and may greatly assist migration to the NG-911 Routing Service) that the PRF support tabular routing per PSAP, i.e., legacy Master Street Address Guide (MSAG)/emergency service number (ESN)-based ANI/ESRK routing for calls arriving without accurate location data.

4.6.5.4 The PRF shall implement policies in the form of rule-sets. The rules shall be of the general form: <action>(<parameters>) as described in NENA 08-003. Some parameters may be variables. Rule-sets shall be stored in the form of XML documents as depicted in RFC 4745.

4.6.5.5 The PRF shall implement variables as described in NENA 08-003. The following variables are explicitly required:

- Date/Time of day
- ECRF query results
- INVITE request URI
- Any SIP header in the INVITE message
- Any XML tag in an INVITE MIME attachment
- Any status variable or presentity values available in a SIP event package, such as QueueState

The PRF should support the use of additional variables in rules that reference status values that are contained within SIP NOTIFY messages. For example, when event packages are added to the SIP Event Function, PRF code changes should not be required in order to reference event values within the new event package. In a similar fashion, PRF code changes should not be required to write rules that reference previously unknown SIP header values. (However, a table of valid variable names or other mechanisms that validate rules is certainly proper; see the requirements of the next section.)

4.6.5.6 The PRF shall be configurable to subscribe to relevant system and destination events for those entities that register with the SIP Event Function. For example, this feature permits downstream ESRPs or PSAPs to inform the PRF of their status (see the nena-ElementState and nena-ServiceState event packages in NENA 08-003) so that the PRF may apply the appropriate rules to the situation.

4.6.5.7 For 911 calls that are treated for normal routing based on the incoming call queue, status variables, and policy rules, the PRF shall query the ECRF to determine the preferred next-hop route. The PRF shall provision at least two ECRFs, e.g., at minimum, a primary and a backup (failover) ECRF.

4.6.5.8 The PRF shall invoke the rule-set associated with the SIP URI returned by the ECRF for final call routing.

4.6.5.9 The PRF shall be implemented in such a way that it will flag, but otherwise ignore, invalid rules in the rule-set, and must always take a default action should it encounter the end of a rule-set without encountering any valid actionable rule, or fail to find a specified rule-set. That is, the PRF must always deliver a call to some PSAP somewhere. Default actions should be configurable, and should generate SIP events and/or SNMP traps to alert monitoring systems.

4.6.5.10 The PRF shall be implemented in such a way that it can detect a logical loop while interpreting policy rules during the processing of a call. If a loop is detected, the PRF must take a default call-handling action.

4.6.5.11 The PRF shall issue a SIP Notify to the SIP Event function should a “notify” rule be encountered.

4.6.5.12 If the PRF is a distinct process from the ESRP, the PRF shall be able to process calls at the same or higher rate than the ESRP call processing rate specified in section 4.6.3.9.

4.6.5.13 Respondents shall list and describe the features of the proposed PRF, with particular emphasis on how the PRF can reliably deliver emergency calls even in the presence of logical problems in the rule-sets or failures in other parts of the NG-911 Routing Service, such as the failure of the SIP Event Function. If

the PRF is a distinct process from the ESRP, Respondents shall explain how high availability of the PRF is achieved per section 4.6.1.1.

4.6.6 PRF Policy Rules Store

4.6.6.1 Respondents shall provide a web-based Policy Store portal that will permit authorized users to view the existing operational rule-sets, and, if the user has sufficient authority, to swap (exchange) specific rule-sets in the operational PRF Policy Store with alternate pre-validated rule-sets. All actions arising from the usage of this web-based portal shall be authenticated and logged per section 4.6.9. The successful Respondent shall document the pre-validated rule-sets prior to system migration. Respondents shall explain the process for incorporating additional rule-sets into the PRF Policy Rules Store.

4.6.6.2 The Policy Store portal of section 4.6.6.1 shall permit users with sufficient authority to submit rule-set additions, deletions, or changes. Such changes must undergo a validation process that includes automated syntax checking and functional review before they are accepted and made available as an alternate rule-set in the list of pre-validated rule-sets. The rules should also undergo a semantic validation process, such as examining the rules for the use of undefined variables, the absence of a final default action, or the possibility of circular references between rule-sets.

4.6.6.3 The web portal to the Policy Store shall be configured to allow access from the MyFloridaNet 911 VRF or from a secure remote VPN appliance in the PSCZ.

4.6.6.4 The Policy Store system shall maintain a log of all changes made to the Policy Store, including the identification of the party making the change.

4.6.6.5 The system shall maintain at least two backup copies of the Policy Rules. These two backup copies shall be located at geo-diverse sites.

4.6.6.6 Respondents shall submit several examples of rule-sets utilized by their proposed solution, and clearly describe the process by which additional rule-sets can be submitted for addition to the production system.

4.6.7 Emergency Call Routing Function (ECRF)

The ECRF is a critical function in the delivery of emergency calls via the NG-911 Routing Service. Respondents shall supply an ECRF function that is at least 99.999 percent available and reliable.

4.6.7.1 The ECRF shall comply with the general requirements of section 4.6.1 above.

4.6.7.2 The ECRF shall comply with RFC 5222 (Location-to-Service Translation [LoST] protocol) and the functional specification of NENA 08-003.

4.6.7.3 The ECRF shall support LoST queries (via TCP) from ESRP(s), PSAP CPE, or any other permitted IP host within the NG-911 Routing Service. The ECRF may rate-limit queries from sources other than provisioned ESRPs.

4.6.7.4 The ECRF shall log all connections, connection attempts, and LoST transactions.

4.6.7.5 The ECRF shall utilize a GIS database that supports the provisioning of all map layers as required in section 4.6.4.10, and which is able to support additional optional map layers that may be populated as part of a future SIF. Respondents shall state any limitations on the number of additional GIS map layers. (A map layer represents the geographical boundaries [polygons] of some service type, such as emergency, law enforcement, fire, ambulance, water rescue, etc., and other data associated with polygons or points on the map, e.g., the URI of the service associated with a polygon or point.) The ECRF shall permit the association of a service request type (as specified in the LoST protocol) to each map layer.

4.6.7.6 The ECRF shall comply with GIS standards including, but not limited to, NENA Standard for *NG9-1-1 GIS Data Model* (draft) and NENA 02-010v9 and NENA 12-014v1.

4.6.7.7 The ECRF shall support updates to the GIS database without disruption of ECRF LoST service. Respondents shall explain how the GIS database update process is able to satisfy this requirement.

4.6.7.8 The ECRF GIS database shall support updates via ESRI shapefiles.

4.6.7.9 The ECRF (or associated administrative program) shall be able to view and validate GIS database changes before they are applied; as an example, and not limited to, detect overlaps or gaps in geographical boundaries contained in a layer.

4.6.7.10 Respondents shall provide a portal or tool that permits the Department read-only access to the GIS database. This function may be rate-limited to avoid impacting emergency call delivery services.

4.6.7.11 Respondents shall state the maximum number of queries per second the proposed ECRF can sustain for at least one minute under adverse but “all up” conditions.

4.6.7.12 Respondents shall describe and list the features of the proposed ECRF, with particular emphasis on how it meets the general requirements of this section (4.6.1 above) and the specific requirements herein.

4.6.8 Location Validation Function (LVF)

The LVF is not a critical function involved in real-time emergency call delivery, but it must be available to call origination providers and to the general public at large so these parties can verify that civic addresses or latitude/longitude will return PSAP or emergency responder URIs. In many ways, the LVF is identical to the ECRF, but because the ECRF must be highly available, it is protected within the Core NG-911 Routing Service security zone. The LVF is available to the general public via an LVF proxy and web portal in the public Internet in the PSCZ, depicted in the security diagram in Exhibit B, and discussed in section 4.7.4.

Respondents are requested to consider future deployment of a state-wide SIF in the design of the LVF proxy and web portal specified below. These access mechanisms might utilize, in whole or in part, an OGC-compliant web feature service. Incorporating an OGC web feature service would provide a standard interface whereby authorized stakeholders could submit and update SIF data across the state of Florida, for subsequent

incorporation into the LVF/ECRF GIS database, as well as a standard means of querying the LVF. While the processes for incorporation of SIF data into the GIS database are not a required feature of this document, Respondents should be aware of the Department's interest in such a capability, and consider leveraging the requirements for LVF access toward this future capability.

4.6.8.1 The LVF shall comply with the general requirements of sections 4.6.1.6 through 4.6.1.11.

4.6.8.2 At least two LVF instances shall be deployed.

4.6.8.3 The LVF shall be a separate instance of the ECRF-like processes running within the Core NG-911 Routing Service security zone.

4.6.8.4 The LVF process shall utilize a separate database instance of the GIS database derived from the ECRF GIS database. Respondents shall describe/show how this separate GIS database instance will be kept synchronized with the ECRF GIS database in real-time or near real-time.

4.6.8.5 The LVF shall be accessed via a proxy server located within the PSCZ. The Core NG-911 Routing Service firewall shall then allow external LVF access only from the proxy process.

4.6.8.6 The LVF shall provide a standard LoST interface via a TCP port. This port may be listed in a DNS entry. Connections and transactions on this port shall be logged and shall be rate-limited by the PSCZ proxy.

4.6.8.7 Respondents shall also provide a user-friendly web server portal located within the PSCZ to which Internet users can browse and manually enter civic addresses or geographic locations along with a service request type. The web server shall query the LVF via the proxy of section 4.6.8.5 and return a user friendly display with the results of the LoST query. An actual map display with the location of the user location is highly desired. This function shall be highly rate-limited, e.g., five queries a day per source IP address.

4.6.8.8 The LVF proxy may also provide a LoST interface accessible by a credentialed connection that may be used by call origination providers or other authorized parties. This port may be used to support a much higher rate of machine-to-machine LVF LoST protocol queries.

4.6.8.9 Respondents shall explain the proposed LVF implementation, with particular attention to the arrangement of the proposed components, user interface and features, and the security aspects of the LVF.

4.6.8.10 Respondents shall provide information on their process whereby ECONs can provide GIS update data and/or report discrepancies.

4.6.9 Logging and Reporting Functions

Extensive logging of NG-911 Routing Service operations is required. All log entries shall be accurately date and time stamped as specified in sections 4.6.1.8 through 4.6.1.10. Only authorized software processes shall have write access to log files. Log files shall be read-only to all other processes and users. Because logs may be subpoenaed and may otherwise become the source of information in legal proceedings, the log system shall be

designed, proposed, and operated with the legal defensibility of log information taken into careful consideration.

Because of the redundant and diverse characteristics required by the NG-911 Routing Service, safely and securely consolidating all log information into centralized log stores is an important consideration. These consolidated log stores provide management information system (MIS) functions rapid and easy location of the desired log data. The MIS system generates tabular and summary statistical reports from the log data.

The NG-911 Routing Service logs shall fall into two categories: transactional logs, which record the routine handling of each and every individual call by various system components, and operational logs, which record status or configuration changes, operator access and interventions, or exceptional events in the operation of the logged component, process, or instance.

Transactional logs provide statistical and detail data important to the administration of the system. They also provide a means to document how any particular emergency call was handled. Transactional logs can also provide important and valuable information when troubleshooting problems in the system, and can sometimes provide early warning when something unexpected is observed.

Operational logs provide a service history of important processes within the NG-911 Routing Service and also a record of who did what to whom and when. Operational logs can be extremely useful in quickly recovering from an operational error, such as a configuration change that had unexpected and unintended consequences, identifying chronic or developing problems, and troubleshooting failures. These logs also provide security, management, and control over the operation of the entire NG-911 Routing Service.

4.6.9.1 All devices in the call flow such as the ESRP, PRF, ECRF, and LNG shall maintain local (dedicated to that instance) "raw" transactional and operational logs. These logs shall contain, at minimum, a process instance identifier, and the date and time-stamped record of each SIP or LoST message processed. Local raw logs shall be maintained for at least 30 days, during which time they shall have been copied to consolidated raw log files for storage for seven or more years.

4.6.9.2 Local transactional logs shall be consolidated into a single consolidated raw transactional file. Local raw operational logs shall be consolidated into a single consolidated raw operational file. These consolidations shall be performed incrementally via an automated process at real-time or at regular intervals, generally not to exceed one hour.

4.6.9.3 At least one copy of the consolidated raw log files shall be maintained at a minimum of two geographically diverse data centers. The consolidation process should alternate between the two sites, and be equipped with sanity checks such that if a failure of the consolidation process fails and destroys, as through a software defect, one of the consolidated raw log files, then that process will halt and an alarm raised, or similar safeguards will protect the undamaged consolidated log files. Respondents may propose alternate mechanisms to ensure the integrity and security of the consolidated raw log files. Respondents shall thoroughly explain the safeguards against the loss of consolidated raw log data.

4.6.9.4 Consolidated raw transactional and consolidated raw operational log files shall be maintained for a minimum of seven years.

4.6.9.5 At all times, authorized Departmental personnel shall have read-only access to the consolidated raw log files.

4.6.9.6 The consolidated raw transactional logs shall, in real-time or near real-time, update a transactional log database. The transactional log database shall order all SIP transactions by the initial time-stamp of the first SIP INVITE, and group related transactions (such as identical SIP Call-id headers) under this initial entry.

4.6.9.7 In the transactional log database, the most commonly utilized SIP headers (To:, From:, Contact:, etc.) and the request URI shall be parsed into dedicated fields into the transactional log database for easy searching and interpretation.

4.6.9.8 Respondents shall provide a consolidated log searching, reporting, and counting tool(s), supporting at least these functions:

- Retrieval of any group of transactions related to a single call identified by time, calling number, source, ultimate destination, or SIP Call-ID header
- Retrieval of a set of calls based on source, ultimate destination, calling number, and conditioned by some specified interval of time
- Generate call volume reports (counts) based on source, destination, call handling (e.g., transferred) over an interval of time

The tool set shall be web-accessible and shall support the creation of new reports based on user-specified selection and output criteria.

4.6.9.9 Respondents shall provide a web portal or other means permitting authorized NG-911 Routing Service administrators read-only access to the transactional log database and log inspection tools. These users shall be able to generate and print their own reports from the data in the transactional log database.

4.6.9.10 All devices, processes or services shall make process and date/time-stamped operational log entries into the dedicated local raw operational log files and into an operating system logging facility (such as the Linux "syslog" or Windows application logs) for the following date and time-stamped events, at minimum:

- Every time the process is started, and any relevant details of how it was started (e.g., command line, monitor program, startup parameters, etc.). This entry (or subsequent entries) should show the startup progress, such as reading configuration files, with a final entry stating the process is "in service" or equivalent.
- Any major change in the process state, such as process going from on-line to standby, shutting down, etc. If possible, a change of process state should be accompanied by a reason, e.g., "operator commanded shutdown," or "memory overflow."
- Significant non-routine events, including "TCP session established by <IP address>," "connection to <process name> lost," "error encountered in config file line xx," "Bad location data with call <call-id>."
- If the process supports operator logins, the operational log should show every login attempt, whether successful, the operator commands issued, and logout.

4.6.9.11 Respondents shall provide a search and report generating tool that can promptly and safely search the consolidated operational logs for all entries or some interval of entries pertaining to a specific device, process, or services, or a specific instance of a process or service. The tool shall also support retrieval of all operational log entries over a specified internal of time, and conditioned for a specific type of entry, keyword, or keyphrase. This tool may operate (via read-only access) on the consolidated raw operational log file, or upon some operational log database derived from the operational log file, at the Respondent's discretion.

4.6.10 GIS Database

The NG-911 Routing Service requires a GIS database to operate. At this time there is no statewide 911 GIS database in Florida. The successful Respondent shall be responsible for provisioning a GIS database adequate to perform location-based routing and to identify the appropriate emergency first responders, e.g., law enforcement, fire, and ambulance, for a location.

Since the GIS data becomes the key dataset for call routing and location validation, the GIS data must be provisioned to the ECRF and LVF. The GIS dataset shall be regularly maintained at the level required to route calls accurately.

The primary GIS layers required for routing and validation are:

- Road Centerlines
- PSAP Boundaries
- Site/Structure Addresses
- State Boundaries
- County Boundaries
- Emergency Service Boundaries (EMS, Fire, Law Enforcement)
- Municipal Boundaries
- Unincorporated Community Boundaries
- Neighborhood Boundaries (subdivisions, gated communities, etc.)

At a minimum, GIS datasets for ECRF and LVF require PSAP and first responder boundaries, and road centerlines. Road centerlines are required for geocoding civic address locations (i.e., city-style street addresses such as 123 Main St) during 911 calls. Centerline road names and address range information must be MSAG-valid.

More detailed address information, such as site structure address location, help pinpoint locations and are highly desirable. The ECRF and LVF queries shall be configured to use a hierarchy of data queries based on the data available for a jurisdiction. Therefore, if GIS data includes site structure locations, the ECRF and LVF shall query that GIS layer first for a civic address match before querying the road centerlines ranges. If there are no site structure points, then the query shall default to geocoding on the road centerline address ranges.

The long-term vision of NG-911 i3 is to provide "sub-parcel polygon features," which can be divided down to building, floor, seat, etc. Respondents should describe if and how their solution would support this fine granularity as data becomes available.

4.6.10.1 Respondents shall describe the hardware and software that will be used to provision a GIS database for the entire state and provide support options for querying neighboring states via an interconnected ESInet. Respondents are not held responsible for inability to interface with non-standard systems in other states.

4.6.10.2 The acquiring or creation of base data and then the maintenance of this data will be performed by the successful Respondent. There are many datasets in Florida at the state and local level, as well as commercially available data. Respondents shall describe how the initial base GIS data will be acquired, validated, synchronized, and updated and the experience the Respondent has performing these functions.

4.6.10.3 The base GIS data must be maintained on a regular basis, and the successful Respondent must provide a process for updates and corrections to be received, validated, and implemented. These requests for change shall be processed within two business days. Respondents shall describe the processes and tools used to perform these updates.

4.6.10.4 The successful Respondent shall maintain, at a minimum, street centerlines; PSAP service boundary layer; and law enforcement, fire, and EMS service boundary layers. Address points shall be added to the database as needed in order to accurately plot civil (street) addresses.

4.6.10.5 All GIS data created or purchased during this contract will become the property of the Department.

4.6.10.6 The MSAG for each county may be owned by the legacy 911 providers in the state. This database must be incorporated into the dataset. Respondents shall describe how this data will be acquired and integrated into the GIS database or otherwise used to perform the proper routing of 911 calls.

4.6.10.7 GIS data being provisioned to an ECRF or LVF shall use the World Geodetic System of 1984 (WGS84) coordinate reference system and datum. GIS data layer replication to the ECRF and LVF shall be established using OGC Web Feature Services. These services will facilitate the exchange of local GIS data formats such as shapefiles, geodatabases, etc. using XML or Geographic Markup Language tags. NENA GIS Data Model 2.0 provides data guidelines and information about XML tags. Additional information on provisioning GIS data and coordinate reference systems is outlined in NENA document 08-003.

4.6.11 Conference Bridging Function

Conference bridges provide one means for NG-911 systems to transfer calls and conduct conferences. NENA Document 08-003 advances several scenarios for implementing conferences and call transfers in an NG-911 system. In some scenarios, bridging is performed by the PSAP CPE, and does not involve NG-911 core functions.

The Florida NG-911 Routing Service shall deploy an IP-based bridging function in the core, and invoke it only when necessary. This solution requires that when an emergency call is to be placed into conference or transferred that the RTP media stream must be moved mid-call. SIP signaling easily provides this capability, and if SIP is able to reliably set up an emergency call, then it can also reliably move the media path mid-call. The changeover usually occurs so rapidly (for voice media) that neither party in the conversation is aware that anything happened. One implementation of this scenario is spelled out in RFC 4579, as well as in NENA 08-003

Section 5.7. Respondents should review the call flow in Exhibit C, items #3 through #6, for a diagramed reference of the call transfer/conferencing scheme.

This purpose of this section is to specify a Core NG-911 Routing Service bridge function suitable for use as described above.

4.6.11.1 Separate conference bridge functions shall be provided for the use of emergency call taker telephones and general administrative telephones; hereafter designated the emergency bridge function and the administrative bridge function.

4.6.11.2 The emergency bridge function provides conferencing features while transferring emergency calls.

4.6.11.3 The emergency bridge function shall support SIP signaling and conference scenarios described in NENA 08-003 Section 5.7. In particular, the emergency bridge function shall support using the SIP REFER method to invite additional parties to the conference.

4.6.11.4 The emergency bridge function shall permit any party to leave the bridge while the remaining parties stay in conference.

4.6.11.5 The emergency bridge function shall permit any call taker to mute the original caller, and/or to temporarily isolate the original caller from the bridge audio.

4.6.11.6 The bridging functions will require access to the PSTN. This PSTN access will be via the Department's existing services. Respondents shall list the recommended number of trunks and the signaling format(s) (e.g., SIP, ISDN, ISUP) and the demarcation point of these trunks.

4.6.11.7 The charges for long distance service shall be passed back to the using PSAP. Respondents shall describe the process and capabilities of the proposed NG-911 Routing Service to document and assign these charges to the user agency or PSAP.

4.6.11.8 The emergency bridging function shall support conference calls of at least six parties in each conference, each party using the G.711 CODEC. The administrative bridge function shall support conference calls of up to 50 parties.

4.6.11.9 The conference bridge function shall support at least the SIP signaling scenario of RFC 4579.

4.6.11.10 Each "all up" emergency bridge function shall support at least as many as 100 separate, but concurrent, voice conferences using G.711, and 10 separate, but concurrent, video conferences using the H.264 video codec, and 10 separate, but concurrent Real-time Text Protocol (RTTP) conferences. This sizing will be reviewed monthly and additional capabilities will be added as needed.

4.6.11.11 The "all up" emergency bridge function shall support at least 400 concurrent voice media connections, 40 concurrent video media connections, and 40 concurrent RTTP conferences.

4.6.11.12 The "all up" administrative bridge function shall duplicate the capacities of sections 4.6.11.6 and 4.6.11.7.

4.6.11.13 The SIP conferencing application shall provide transactional logging and the exchange of SIP location conveyance and other MIME attachments.

In addition to the requirements listed above, Respondents should highlight any distinguishing aspects of their service to be considered during the evaluation for the NG-911 Routing Service.

The remainder of this page is left blank.

4.7 Operational Requirements

4.7.1 General Operational Requirements

4.7.1.1 The successful Respondent shall cooperatively develop an Operations Guide for the operation of the NG-911 Routing Service with the Department. This will serve as a guide of how to provide these services and clarify the procedures of the contract. An example Operations Guide is included in Exhibit F of this document to demonstrate the comprehensive and detailed nature expected of this document. The Operations Guide should include, at a minimum, the following:

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

4.7.1.2 The successful Respondent shall cooperatively develop a User's Guide for the operation of the NG-911 Routing Service with the Department. This will serve as a guide of how customers will interact with the NG-911 Routing Service. The User's Guide should include, at a minimum, the following:

- Mission Statement
- Types of Services
- Optional Services
- Change Management
- Data Management
- Trouble Management Support
- Escalation Procedures
- Major Outage Process
- Ordering NG-911 Routing Service
- Billing
- NG-911 NMS Tools
- Security

- SLAs
- Hours of Operation

4.7.1.3 Respondents shall include a list and summary of each service they provide that will contribute to the provisioning of the NG-911 Routing Service solution as specified in this document. These descriptions may, at the Respondent's discretion, include the Respondent's marketing names and Respondent's descriptions of the services. Regardless, each description of a service must make clear how that service relates to and satisfies the functions specified in this document.

4.7.1.4 Respondents shall include a summary of *optional* services offered by the Respondent that would *enhance* the provisioning of the NG-911 Routing Service described in this document. These may include the Respondent's marketing names and Respondent's descriptions of the services. Each optional service must be accompanied by an explanation of how that optional service would enhance the NG-911 Routing Service. This SHALL NOT be a list of all services provided by the Respondent, but limited to those optional services that, in the Respondent's view, would enhance the NG-911 Routing Service.

4.7.1.5 All e-mail and web addresses will be required to use the Florida named domains as provided by the Department.

4.7.1.6 As described in this document, the NG-911 Routing Service is complex and requires a great deal of activities to function properly. Respondents shall describe all operational activities that will be needed to support the proposed solution, and the frequency of these activities. This description will demonstrate that the Respondent has a clear understanding of the operations of the NG-911 Routing Service.

4.7.1.7 The successful Respondent must provide regularly scheduled written documentation concerning operation, monitoring, and maintenance activities. These reports will include SLA, traffic, and activity reports. Respondents shall describe the types of reports available and shall provide examples.

4.7.1.8 Recurring coordination is required to manage the service. The successful Respondent will be expected to schedule monthly engineering meetings with the Department. Respondents shall describe agenda items that the Respondent would expect to cover in these meetings.

4.7.1.9 The NG-911 Routing Service requires many types of data to operate. As a result of this process, the Department will be contracting for this data to be created and used, and as a result all data will become property of the Department. Respondents shall describe the major types of data, such as GIS Centerline, ESN, Policy Routing Store, etc., used by the proposed NG-911 Routing Service, and shall describe the process used by the Respondent to collect, validate, and maintain this data.

4.7.1.10 The NG-911 Routing Service requires detailed design and engineering during the implementation phase and throughout the operation of the service. Respondents shall describe the types of support, hours of operations, and descriptions of the qualifications for each role in this process.

4.7.1.11 Changes and new services for the NG-911 Routing Service shall be tested in a laboratory or test environment prior to deployment on the production environment. The test environment shall be made available to the Department. Respondents shall describe the test systems in detail, including the physical location(s) of the test environment, the methods by which it models or mimics the operation of the production system, the extent to which the test environment duplicates some or all of the production environment, and any known limitations of the test environment compared to the production environment, e.g., those aspects of the production environment that the test environment does not model. The availability of testing tools such as traffic generators, device simulators, and automated test suites should be included in this description. The Department will inspect the laboratory/simulator system and will witness tests of major upgrades before authorizing upgrades on the production system. Witnessing tests may be by physical presence in the laboratory and/or by remote access to the test system by approved Department personnel.

4.7.1.12 The successful Respondent is required to support the NG-911 Routing Service 24x7. This staffing is needed to operate the NG-911 Routing Service; overtime is not allowed for any operational activities of the NG-911 Routing Service during planning, implementation, or operation. In addition to the staffing worksheet listed in requirement 4.4.1.22, Respondents shall describe the availability of the following roles, to include Respondent staff or sub-contractors, response times, and locations, at a minimum:

- Field Responders
- NOC (Tier 1)
- Tier 2 Technicians
- Tier 3 Engineers
- Executive Escalation

Note that section 4.4.1.22 requires a specific staffing plan for the migration/cutover phase of the project. The response to section 4.7.1.12 should indicate differences between the staffing required during migration/cutover operations and the staffing required to support daily operations of the NG-911 Routing Service post cutover.

4.7.1.13 In addition to the NOC functions, the successful Respondent will provide a help desk to assist users with questions and minor changes, such as resetting passwords. This function may be a part of the NOC itself or a separate entity. This service shall be provided for unlimited support calls without additional charges.

4.7.1.14 The NG-911 Routing Service will require maintenance personnel and users to access various services within the system. The security of these systems is critical to the service. Respondents shall provide written documentation on how remote maintenance and on-site maintenance will satisfy DMS Rule 60FF.

4.7.1.15 All data used in the NG-911 Routing Service is required to be backed up. While all services are mirrored and located in geo-diverse sites, each site must have a data backup and recovery plan. Data backups must be stored at separate, secure off-site locations. Respondents shall describe the proposed process used to accomplish this.

4.7.1.16 The NG-911 Routing Service and stakeholders will have third-parties, such as call origination providers, wireless carrier mobile positioning system providers, and PSAP CPE vendors, which may impact or have a role in the NG-911 Routing Service. The successful Respondent must cooperatively work with the Department to determine which third-parties will be involved and the best method for coordination, including whether coordination should go through the Department, the customer or the contractor, and which parties should be informed of the coordination.

4.7.2 Monitoring, Alarming, and Trouble Reporting

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

4.7.2.1 Monitoring shall include all existing MyFloridaNet capabilities, including those outlined in section 4.0.4. It shall also include NG-911 Routing Service specific monitoring, including:

- Call delivery performance
- Call media quality, such as Mean Opinion Scores (MOS) and talker echo levels for voice media
- Fault monitoring for each component or instance of an NG-911 Routing Service function
- SLA compliance monitoring
- Security violation alerts
- Unusual traffic or error trend thresholds, such as unusual overflows, unusually low call volume, repeat calls/call attempts from same source, or frequently missing or defective location data
- Overall NG-911 Routing Service health

4.7.2.2 The voice quality of the NG-911 Routing Service shall be explicitly monitored via periodic automated probing of the network from various ingress to egress demarcations, or points close to the demarcations. Alternatively, Respondents may propose other schemes for voice quality monitoring that will provide equivalent or superior information. The prime metrics are the MOS and talker echo as described in ITU-T document G.131. The MOS should be measured using methods known as "Perceptual Evaluation of Speech Quality," as described in ITU document P.862E. Talker echo must also be periodically sampled. Although most echo problems will originate outside of the NG-911 Routing Service, the NG-911 Routing Service shall deploy adaptive digital echo cancelation in PSTN - VoIP media gateways, and at other strategic locations in the system to control talker echo problems. See Exhibit G for examples of expected voice quality monitoring.

4.7.2.3 Voice quality complaints shall be promptly investigated and the cause determined so far as possible. In a properly designed and deployed NG-911 Routing Service, most voice quality complaints will originate from root causes outside the of the NG-911 Routing Service itself. However, the Department shall require the successful Respondent to be contractually obligated to continuously demonstrate that the cause of voice quality issues is external to the NG-911 Routing Service, and to work tirelessly with the appropriate stakeholders to assist them in resolving voice quality problems.

4.7.2.4 The NG-911 Routing Service requires an effective process for continuous monitoring and reporting; this begins with establishing a methodology that includes monitoring, analyzing, reporting, and

responding to all components and functions of the NG-911 Routing Service. Respondents shall describe the devices, services, and functions that the proposed NG-911 Routing Service will monitor.

4.7.2.5 Monitoring

4.7.2.5.1 The successful Respondent will monitor all application, processes, or service instances required to provide NG-911 Routing Service to customers. Examples of parameters that may or should be monitored (depending on the process or service functional details) include the following:

- Current status of monitored element: Working/In-service, Failed/Out-of-service, Idle, Busy, Down for Maintenance, etc.
- CPU usage over time interval (typically five minutes)
- Memory/Disk space usage
- Bandwidth or Input/Output packet flow rates
- Traffic/Transaction rates over time interval
- Percentage of errored transactions over time interval
- Presence information/alarms

Maximum and/or minimum alarm thresholds should be set on the various monitored parameters as appropriate for the function and characteristics of the each process or service instance.

4.7.2.5.2 The signaling, voice quality, and measured parameters of sections 4.7.2.1, 4.7.2.2, and 4.7.2.5.1 shall be reported and provided in a dashboard format. The dashboard will provide, at minimum, the following information:

- Overall service health
- Signaling Performance/Current Call Volume
- Current voice quality averages
- Problem alerts and indicators

4.7.2.5.3 The successful Respondent will coordinate with the MyFloridaNet monitoring and reporting systems to monitor the connectivity between sites. The successful Respondent must also coordinate with the Department to allow access to the Respondent's monitoring systems by the Department and customers.

4.7.2.5.4 Monitoring shall be a combination of manual and automated processes that are consistent and repeatable. Systems that are capable of event logging should do so. Other methods such as scanning and gathering performance data will be incorporated to provide a complete method for identifying anomalies in real-time or near real-time. Monitoring should capture events that may indicate malicious activity, deviations from policy and procedures, system failure, and flaws in logging mechanisms. Monitoring is required to capture atypical activity as well as validate normal network functionality. The degree of system logging and monitoring should provide balance between gathering meaningful information and impacting operational efficiency.

4.7.2.5.5 The successful Respondent will deploy monitoring that will provide the following:

- Collect, correlate, and provide the ability to analyze system information
- Provide current situational awareness of all systems across the network
- Raise warnings or alarms of failed or failing components or process instances

- Provide warning and the ability to proactively manage threats and threat activities
- Assess effectiveness of security controls

4.7.2.6 Analyzing

4.7.2.6.1 The successful Respondent must establish a scheduled routine to analyze events in order to provide the ability to respond in a timely manner. Anomalies must be analyzed to determine impact to normal operations. Determination for appropriate actions will be made and actions should be consistent with MyFloridaNet processes.

4.7.2.6.2 Proper analysis provides insight to the overall effectiveness and current state of control measures in place as well as the health of the network, attached devices and applications. The analysis of system logs, scanning and other data collected should provide information allowing the source of an event to be traced to one or more factors causing the event, such as the following:

- Failure of current controls
- Missing controls
- Insufficient strength of controls
- Increase in the capability of a threat source
- Decrease in system performance

4.7.2.7 Reporting

4.7.2.7.1 The successful Respondent must coordinate regularly scheduled reporting procedures. These procedures must be documented and a consistent methodology utilized. Reports may be required on a daily, weekly, monthly, or quarterly basis as appropriate. Reports of critical concern, such as system outages, must also be documented. Reports should provide adequate information to support findings or recommendations. Reporting is required to be consistent with the MyFloridaNet reporting process. Reports may provide information to achieve the following:

- Demonstrate the state of the information systems
- Validate efficiency of applications, equipment and controls
- Verify compliance with local, state and federal policies, regulations and mandates
- Maintain awareness of threats, vulnerabilities and system functionality

4.7.2.8 Responding

4.7.2.8.1 The successful Respondent must have a documented procedure for responding to an imminent threat. Whether the threat originates from equipment failure or a computer virus, the response needs to be commensurate with the severity of the event. When the situation has been mitigated, the process of reporting and determining additional actions should continue until a permanent resolution is implemented. Responding may include the following:

- Initiation of corrective action
- Reassessment of the current operating environment, controls, configurations, or requirements
- Modification of or update to the current operating environment, controls, configurations, or requirements
- Reassessment of current monitoring or reporting thresholds

4.7.2.9 Publishing/Sharing Information

4.7.2.9.1 The MyFloridaNet monitoring tools allow for full read-only CLI and GUI access to all tools and data for the Department. This is critical for the SUNCOM NOC. These tools are also available to customers with appropriate scope of view and command. Customers' access is limited to tools and components of the system that are directly utilized by the customer. The NG-911 Routing Service tools and processes shall grant the same functionality and access.

4.7.2.9.2 The successful Respondent shall offer access to operational services and tools to the Department, customer and call origination provider staff using web-accessible interfaces using a standard web browser. Public Internet access from home 24x7 is required. Single sign-on for the entire suite of services is required. A common NG-911 theme is displayed.

4.7.2.9.3 Respondents shall describe the tools and processes used by the Respondent to monitor and manage the proposed NG-911 Routing Service. For each tool or process, Respondents shall describe, at minimum, the following:

- Name of tool or process
- Developer (software company or manufacturer)
- What is monitored by the tool or process
- Examples of how it reports the information monitored
- Methods of access (web, e-mail, special device)
- What systems or devices are monitored
- Ability to filter access to users, devices, or processes
- Screen shot examples for each tool

4.7.2.9.4 A fundamental requirement of VoIP telephony measurement tools is the ability to establish logical partitions of the NG-911 Routing Service that will be defined as dedicated views for specific PSAPs. The Department, NG-911 Routing Service customers, and successful Respondent management staff share management tools. The Department requires view access to the same parameters the successful Respondent uses to manage the statewide NG-911 Routing Service. The Department requires a global view of tools, core equipment and services and any Respondent-managed CPE. Telephony measurement tool views permit each PSAP to view their individual service domain. PSAPs are not able to view other PSAP domains unless authorized. Retention time of monitoring information should generally be one calendar year unless otherwise negotiated.

4.7.2.9.5 A trouble reporting and tracking system is required. Trouble reporting must allow customers to report issues, at a minimum, by phone, by e-mail, or via a web portal. Customers and the Department shall be able to access a web-based system to follow and display all history and activities associated with a trouble ticket. Respondents shall describe the system that is proposed.

All tickets and associated data must remain available for viewing for the term of the contract. At contract expiration, the successful Respondent shall provide the Department a data dump of all trouble tickets and history that occurred during the contract.

4.7.2.9.6 Respondents shall describe the escalation procedures that will be provided to the Department. This shall include names, titles, escalation role, company role, availability, and contact instructions.

4.7.2.9.7 Planning is a major part of providing any service effectively. The NG-911 Routing Service will require several levels of plans to be developed by the successful Respondent and approved by the Department. Respondents shall describe the process used to develop and manage the plans need to operate this system and shall describe the successful development of similar plans and provide examples. The following plans are required at a minimum:

- Strategic Plan – This is a high-level plan for the implementation, operation, update, and upgrade of the NG-911 Routing Service. This plan establishes the goals and objectives to be accomplished. This is a minimum of a 5-year plan, which is updated annually or more often if needed.
- Tactical Plans – These are specific plans to accomplish the goals and objectives of the strategic plan. These are usually short-term, e.g., the deployment of a new service.
- Education Plan – This describes the plan established to provide education to the public on the use of the system.
- Training Plan – This describes the plan established to provide education to telecommunicators, PSAP and Department administrators, and others as required in sections 4.1.23 and 4.1.24.
- Communications Plan – This describes the methods and messages for communicating with various stakeholders and others required to successfully operate the NG-911 Routing Service. This can be included in other plans, but must be developed.
- Risk Management Plan – This describes the known or potential risks, both positive and negative, to the NG-911 Routing Service. Each risk is defined, measured for impact, and mitigation steps defined.

4.7.2.9.8 The successful Respondent will work cooperatively with the stakeholders to develop the public education plan and will be involved in delivering messages during the deployment and operation of the NG-911 Routing Service. The successful Respondent will also provide materials and staff for presenting these messages as coordinated with the Department. Respondents shall describe where and how the Respondent has performed this type of service in the past.

4.7.2.9.9 The mission critical nature of any 911 system requires planning for failures and disasters. Respondents shall define the process used to respond to and manage failures of portions or the whole of the NG-911 Routing Service. These processes will be expected to be tested on a regular basis, such as failing a data center. The Department is specifically interested in the following plans:

- Continuity of Operations (COOP) – This is the plan and process used to continue the operation of the NG-911 Routing Service with limited failures in the system.
- Disaster Recovery – This is the plan and processes to recover from a failure to normal operational states.

4.7.3 Change and Configuration Management

Changes to configurations will be managed through an established change management process. Current and recent past configurations must be documented and maintained. The successful Respondent must establish a system for safely implementing, documenting, and maintaining the configurations of hardware devices and software applications as necessary to provide consistent versions throughout the operating environment. Benefits gained from configuration management include safety, ease of use, ease of maintaining, ease of troubling shooting problems when they arise, and straightforward and rapid back-out should an unexpected

problem arise. The process begins by establishing a baseline configuration and extends through monitoring the change management process to assure compliance.

4.7.3.1 Configuration Management Database (CMDB)

4.7.3.1.1 The successful Respondent shall provide and maintain a CMDB, which shall contain an inventory of the hardware and software process instances in the system, including items required in section 4.7.3.2 below.

4.7.3.1.2 The CMDB shall preserve historical configurations, including, at minimum, the two previous operating configurations.

4.7.3.1.3 The CMDB shall reside within the Core NG-911 Routing Service security zone.

4.7.3.1.4 A backup copy of the CMDB shall be maintained at a geographically diverse location, and the backup copy shall be synchronized with the CMDB at least daily.

4.7.3.1.5 A tool shall be provided that permits quick and easy comparison of recent configurations for a specific device or a specific process instance, and which highlights the differences between the configurations.

4.7.3.1.6 A reporting tool shall be provided that can filter and sort the CMDB contents by the contents of specified fields within CMDB records, such as the device or software type, by location, or by version number.

4.7.3.2 Initial Deployment Configurations

4.7.3.2.1 The successful Respondent shall establish a methodology for naming configuration data for each device or process, which conforms to Department device naming and addressing guidelines.

4.7.3.2.2 The successful Respondent, in cooperation with the Department, shall inventory and identify the hardware and software that must be included in the configuration management process. Each device or software so identified shall be added to the CMDB described in section 4.7.3.1 above. Examples of devices recorded in the CMDB include routers, switches, servers, workstations, gateways, firewalls, and SBCs. Examples of software processes include operating systems, SIP proxies, NIF or PIF programs, ECRF processes, monitoring applications and tools, web portals, and authentication software. Any process that requires a configuration and/or license shall be inventoried in the CMDB.

4.7.3.2.3 Initial data associated with each entry in the CMDB shall include attributes such as the following:

- Installed operating system/firmware name/identifier and version
- Installed application names/identifier and version
- Applied patches
- Device serial number and location building, row, rack, and shelf
- Subject matter expert contact information responsible for testing configuration or changes
- Device or software console/management port DNS name or IP address and port number

4.7.3.2.4 Baseline or initial configurations shall comply with these principles:

- Comply with Department device naming and addressing guidelines

- To the degree possible, the initial configuration for each device or software shall be rendered into a standard template across all devices of similar type or role
- Employ hardening steps such as disabling of unused interfaces and services, disabling local administrator rights, removing default user names and passwords, and generally deploying the most restrictive configuration consistent with the operational requirements
- Utilize best practices for operating system hardening, such as the National Institute for Standards and Technology (NIST) guidelines or the International Organization for Standardization (ISO) 27002 standards
- All configurations must meet requirements as set forth by the Department

4.7.3.2.5 The successful Respondent shall supply an automatic configuration backup tool, which will automatically store current configurations in the CMDB. Ideally the initial configurations will be entered into the CMDB by this automatic configuration backup process.

4.7.3.3 Change Process

4.7.3.3.1 When a need for a configuration change is identified, the requesting parties shall submit a change request form, or make the request by another means as specified by the successful Respondent and agreed to by the Department. The change request form should identify:

- Reason for the change
- Nature of the work to be done
- Devices and/or processes affected
- Likely impacts of the change while change is being installed
- Requested time the change will be deployed
- Method used to verify the change has been successful
- Back-out process if the change does not go as anticipated

4.7.3.3.2 In most instances, and particularly for major changes, the change shall be pre-tested on the laboratory/test environment described in 4.7.1.11. Test results should be made available to the change review process.

4.7.3.3.3 All change requests shall undergo a review process involving the successful Respondent (or parties with SLA responsibility) or their representatives and the Department or their representatives. The review process should particularly watch for change requests that may be incompatible with some currently in-service hardware or software levels, e.g., have all pre-requisites been satisfied. If there is agreement to proceed, the review committee should ensure appropriate notification of affected or potentially affected stakeholders is accomplished in a timely fashion prior to the change.

4.7.3.3.4 In an emergency, the SLA responsible party may approve an immediate change and inform the review committee within two business days of the action taken.

4.7.3.3.5 The change shall be implemented per the schedule approved by the review process.

4.7.3.3.6 If the change is successful, documentation and/or the CMDB shall be updated. (This may be an automatic process.) If the change is not successful, the back-out procedure shall be followed, the

affected components verified as returned to service, and the review committee shall be notified and shall determine the appropriate next step.

4.7.3.4 Maintain CMDB

Many changes will result from the growth of the ESInet and the addition of PSAPs, ECONS, and additional devices and process instances to the operating NG-911 Routing Service. Once the NG-911 Routing Service becomes operational, additions and deletions to the system should essentially follow the change process of section 4.7.3.3 to ensure the safety of the operating portion of the system.

4.7.3.4.1 Additions to the system shall be deployed utilizing the current baseline configurations as described in section 4.7.3.2

4.7.3.4.2 Additions to the system shall be consistent with the change management process as described in section 4.7.3.3. However, pre-approval for standard operating procedures may be utilized in lieu of the individual case-by-case process of change review described in section 4.7.3.3.

4.7.3.4.3 It is imperative that additions to the system be included in the CMDB inventory and that all system documentation be properly maintained.

4.7.3.5 Monitor and Audit the Change Management Process

4.7.3.5.1 The successful Respondent shall verify that the automatic configuration backup process is functional and current at least monthly. One validation technique could be to re-initialize a device to a factory default state, restore the configuration from the CMDB, and then verify that the device has been fully restored.

4.7.3.5.2 The successful Respondent shall review the established change management process and report on compliance with the process at least annually.

4.7.3.5.3 The successful Respondent shall audit the CMDB for deficiencies and inconsistencies at least annually.

4.7.3.5.4 The CMDB audit must include the following:

- Ensure the inventory of all hardware devices and software applications in the operating environment is complete and accurate.
- Compare a sample of configurations for various devices and processes to the current configuration templates, and investigate discrepancies or update the templates as appropriate.
- Review system documentation, including process documents such as standard operating procedures, for accuracy, completeness, and currency. Corrections shall be implemented by the successful Respondent via the established change management and configuration maintenance process.

4.7.4 Security

4.7.4.1 The NG-911 Routing Service shall use a layered security approach with defined and protected network boundaries. The NG-911 Routing Service shall integrate and comply with security processes and requirements of DMS Rule 60FF-1 to 3 and 60FF-6. Respondents shall provide narrative and diagrams

detailing the network points of ingress and egress, as well as address remote access of the NG-911 Routing Service, to include, at a minimum, the following:

- Network defense for all zones of the NG-911 Routing Service
- Next generation IPS to be placed at egress and ingress points between security levels
- Reputation-based protection with frequent updates (two hours) at points of ingress
- Rate-limiting
- Application classification and filtering
- Data leak prevention
- DDOS protection
- Botnet remediation and protection

4.7.4.2 Cyber Security Zones

The NG-911 Routing Service shall be divided into distinct security zones. A zone is an interconnected set of IP subnets within which IP packets may be freely exchanged among connected IP hosts and gateways. Unless otherwise noted, the perimeter of each security zone shall be protected via next generation firewalls from interconnected adjacent security zones. The diagram in Figure 31 (a duplicate of Figure 21) shows the relationships among the security zones as described below.

At minimum, the following security zones shall be established:

1. Public Internet – The public Internet represents a zone with no security mechanisms, and shall be viewed as a source of extreme security threats. However, the NG-911 Routing Service must support the ingress of emergency calls from the public Internet via NENA i3 signaling formats. The public Internet may also be used to obtain status information about the NG-911 Routing Service, and for authorized personnel to remotely access, manage, and maintain certain aspects of the NG-911 Routing Service. The operators of networks capable of originating emergency calls (ECONs) may also utilize the public Internet to access services within the PSCZ (such as the LVF) and other information required to support the delivery of emergency calls to the NG-911 Routing Service.

   Respondents shall utilize MyFloridaNet for interconnection to the public Internet. (Section 4.1.5) MyFloridaNet offers redundant, managed, and monitored Internet service with all of the tools and capabilities described in section 4.0.4.2.

2. Public Security Control Zone – PSCZ is a security zone that connects to the public Internet on one side and the Core NG-911 Routing Service on the other side. Any IP traffic to or from the public Internet and accessing the NG-911 Routing Service must terminate on application gateways in this security zone. No direct IP access to the NG-911 Routing Service from the public Internet shall be permitted. Indirect application gateways shall be provided in the PSCZ that support controlled access to the NG-911 Routing Service from the public Internet. For example, a SIP B2BUA SBC shall be located within the PSCZ, which will terminate a SIP call originating from the public Internet on one side and re-originate the SIP call on the other side toward the NG-911 Routing Service. This public Internet SBC shall be a separate and physically distinct device from other SBCs used in the NG-911 Routing Service.

The perimeters of the PSCZ shall be protected by next generation IPS firewalls as described in detail in this section and in section 4.3.3. The firewall connecting the PSCZ to the public Internet shall be a physically distinct and separate device from other firewalls in the system.

A basic policy of PSCZ firewall configurations is that direct communication from the public Internet to/from the Core NG-911 Routing Service security zone is not permitted. Rather, the Internet firewall will permit Internet communication with only one side of the SBC, while the NG-911 Routing Service firewall will permit communication only between the other side of the SBC and the Core NG-911 Routing Service security zone.

In a similar fashion, web servers that provide NG-911 Routing Service status information to the Internet and remote administration servers terminating VPNs that support remote administration and support of the NG-911 Routing Service may be deployed in the PSCZ. Again, the perimeter firewalls shall support only connections between the Internet and PSCZ servers on one side, and the Core NG-911 Routing Service on the other side, but never a direct connection from the Internet to the Core NG-911 Routing Service security zone. For example, if a contractor wishes to apply a patch to a process running in the Core NG-911 Routing Service security zone via the public Internet, it would be necessary for that contractor to first upload the patch to a jump server via a VPN, and then to command the jump server to forward the patch to the appropriate destination within the Core NG-911 Routing Service security zone. The remote administration server and firewalls shall apply security rules and perform logging functions as described below.

3. Core NG-911 Routing Service Zone – This security zone will observe the highest levels of security. Instances of the ESRP, ECRF, PRF, and other functions critical to the overall delivery of emergency calls shall be located within this security zone. LNGs that terminate incoming 911 traffic from legacy trunks (such as SS7 ISUP or CAMA trunks) shall also be located within this zone.

4. MyFloridaNet DMZ – Critical services and processes that are used by PSAPs, sub-state or other state ESInets, administrators, or other entities that utilize the MyFloridaNet 911 VRF shall be located in the MyFloridaNet DMZ. For example, DNS, emergency call logging functions, Tier 2 NTP servers, or GIS database application servers that are shared among PSAPs shall be located in the MyFloridaNet DMZ. The Department desires that the call conference bridges (section 4.6.11) also be located in this security zone. The MyFloridaNet DMZ may be a port on the Core NG-911 Routing Service to MyFloridaNet 911 VRF firewall.

5. MyFloridaNet 911 VRF Security Zone – This routing domain is the MyFloridaNet IP infrastructure (WAN) that interconnects the Core NG-911 Routing Service security zone with PSAPs, sub-state or other state ESInets, and native NENA i3 ECONs. This security zone operates at a high-level of security that does not unduly restrict the use of the MyFloridaNet 911 VRF for public safety applications between PSAPs and sub-state ESInets as well as emergency call delivery. Each interconnection with the MyFloridaNet 911 VRF security zone shall be protected by a next generation IPS firewall.

6. Extranet, Sub-state, and External Security Zones – These are private IP networks operated by ECONs, PSAPs, sub-state entities, or other state ESInets that interconnect to the MyFloridaNet 911 VRF for the purpose of the delivery of emergency calls to or from the NG-911 Routing Service in NENA i3 formats. While these networks should be secure, they shall be considered untrustworthy by the Florida NG-911

Routing Service. These security zones shall interconnect to the MyFloridaNet 911 VRF or the MyFloridaNet DMZ by either a next generation IPS firewall or via a B2BUA SBC, as agreed to by the interconnecting entity and the NG-911 Routing Service successful Respondent. An SBC will likely be required if interconnections are required between the interconnecting entity's private IP network and the Florida NG-911 Routing Service. For example, an SBC may be used to resolve IP addressing conflicts, convert from IPv4 to IPv6, or resolve differences in SIP signaling. An example of a potential SIP signaling issue is that the Florida NG-911 Routing Service requires support for the SIP "Replaces" header. If the interconnecting entity does not support "Replaces," then an SBC may perform this conversion. Note that any SBC used for this purpose must be a separate SBC from the Internet SBC mentioned in the PSCZ discussion above, but the SBC used to connect to private IP networks may be shared for several such interconnections.

The remainder of this page is left blank.

NG-911 Routing Service Security Diagram

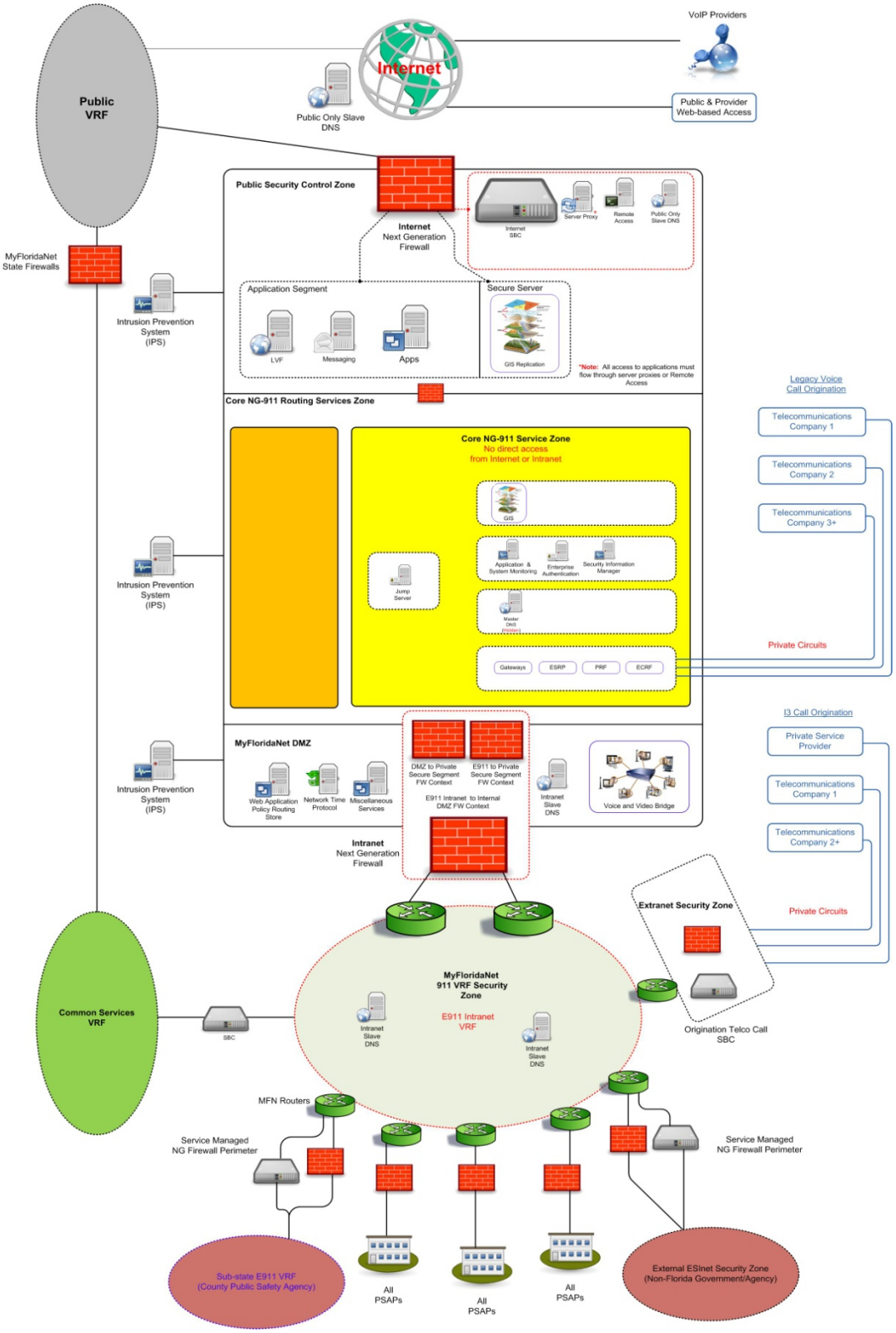


Figure 31—Security Zones

Return to Index

4.7.4.3 Respondents shall describe their method for security management and the subsequent functions of security required to deter intentional or unintentional events from causing an interruption of service or the loss of data. Respondents shall include in their description, at a minimum, the following methods to:

- Categorize the impact of a risk as low, moderate, or high
- Select security controls including the name of the controls selected
- Implement security controls
- Assess effectiveness of security controls
- Authorize system access
- Monitor the environment
- Integrate and comply with MyFloridaNet and local authorities

4.7.4.4 Respondents shall provide a layered security plan for the data center: Internet, intranet, internal segments, network, host, and applications.

4.7.4.5 Respondents shall describe their system update and the patching strategy which assures systems are kept up-to-date with current versions and patches.

4.7.4.6 The NG-911 Routing Service shall use centralized authentication utilizing dual authentication that shall include RADIUS with user accounting (logging all changes per user) for all devices. Identity providers shall insist on two factor authentication of agents and make use of systems such as the following:

- Passwords, which must conform to local password policy
- Trusted Digital Certificates (Certs)
- Tokens (RSA SecureID)
- Key Fob
- Smart Cards conforming to ISO/IEC-7816 (1-15)
- Biometrics, including fingerprints, palm prints, retina scans, face recognition and voice recognition

4.7.4.7 Access Control (Access, Authentication, and Authorization) access to all devices, applications and data shall require uniquely identifiable credentials, centrally authenticating individual users, devices, or systems prior to granting access. Respondents shall describe the strategy for each type of access.

4.7.4.8 Each agency and each agent in an agency shall be issued credentials that allow them to be identified to all services in the NG-911 Routing Service. This will include the successful Respondent, Department, PSAP, and sub-state ESInet authorized personnel. There shall not be any shared credentials such as "admin" allowed. When authenticating within the NG-911 Routing Service, an agent or agency shall assume one or more roles. The roles that an agent or agency may assume are limited by policy of the immediately superior agency. Respondents shall describe the process to authenticate and manage all users.

4.7.4.9 Services within the NG-911 Routing Service shall implement a single sign-on paradigm.

4.7.4.10 Passwords or passphrases shall have a minimum of eight characters consisting of at least three of the character sets: uppercase, lowercase, numeric, and non-alphanumeric characters shall be used.

Respondents shall describe how the NG-911 Routing Service will establish and monitor password complexity and use, to include the ability to identify and respond to failed login attempts.

4.7.4.11 The NG-911 Routing Service shall protect all data associated with the operation of the NG-911 Routing Service. This includes, but is not limited to, configurations, databases, or logs. Data must be protected in devices connected to the system in staging, or copied to another location, such as off-site backups or testing laboratories. Respondents shall describe methods to protect data from malicious software, leakage, and modification as well as guaranteeing delivery of emergency calls.

4.7.4.12 Respondents shall provide monitoring and reporting systems such as IPS to identify and monitor security incidents, unusual network activity, e.g., malicious traffic. Monitoring and reporting shall be commensurate with the level of security at each segment.

4.7.4.13 Respondents shall provide SIM, a security intelligence platform that provides a unified architecture for collecting, storing, correlating, analyzing and querying log, threat, vulnerability and risk-related data.

- All routers, firewalls, IPS, switches, servers, proxies involved shall log to the E911 SIM.
- Sensors should be located on each network security segment.
- Respondents shall integrate with MyFloridaNet's current SIM to share information.

4.7.4.14 Respondents shall provide staff to monitor and respond to all security issues. This includes responding to DoS attacks or just a password reset for users. These security-qualified staff shall be part of a 24x7 dedicated monitoring system.

4.7.4.15 Respondents shall provide active protection to the NG-911 Routing Service, such as IPS and anti-virus software, which is kept current and monitored.

4.7.4.16 Respondents shall provide testing and audits of all security systems to include, at a minimum, the following:

- Component acceptance testing
- System-wide acceptance testing
- Yearly penetration testing from Internet, intranet, and extranet
- PSAP testing
- Quarterly audits for all hosts involved in E911
- Compliance audits and reviews

4.7.4.17 Physical access control shall be employed to assure all information resources are physically secured and protected from theft, misappropriation, misuse, unauthorized access, and damage.

4.7.4.18 Authorized physical access to the NG-911 Routing Service components shall be restricted to approved personnel who have completed background checks required by the State of Florida Statute 110.1127.

4.7.4.19 Storage media and output of a sensitive nature shall be stored, handled, and disposed of in a manner commensurate with sensitivity level. Respondents shall describe how the following will occur:

- Storage and output shall be kept from disclosure to non-authorized personnel.
- Disposal of sensitive hard copy or printed material shall be shredded.
- Disposal of electronic devices shall be degaussing, magnetic media erasing, disintegrator or method to assure sensitive data is completely removed and un-retrievable.

4.7.4.20 All equipment and data communications network sites shall be physically secured and restricted to authorized personnel.

4.7.4.21 The NG-911 Routing Service shall provide secure remote access for the purpose of monitoring, troubleshooting maintenance, and repair of the system including software updates and patches. This access shall not be from direct access from a device outside of the NG-911 Routing Service, but shall make use of a VPN connection to a jump server (located in the PSCZ) as depicted in the diagram below. The VPN connection software shall include validation of the remotely connecting (Technician's) computer, including that it has required versions of anti-virus software installed and meets authentication requirements. Respondents shall describe how the system will perform this remote access.

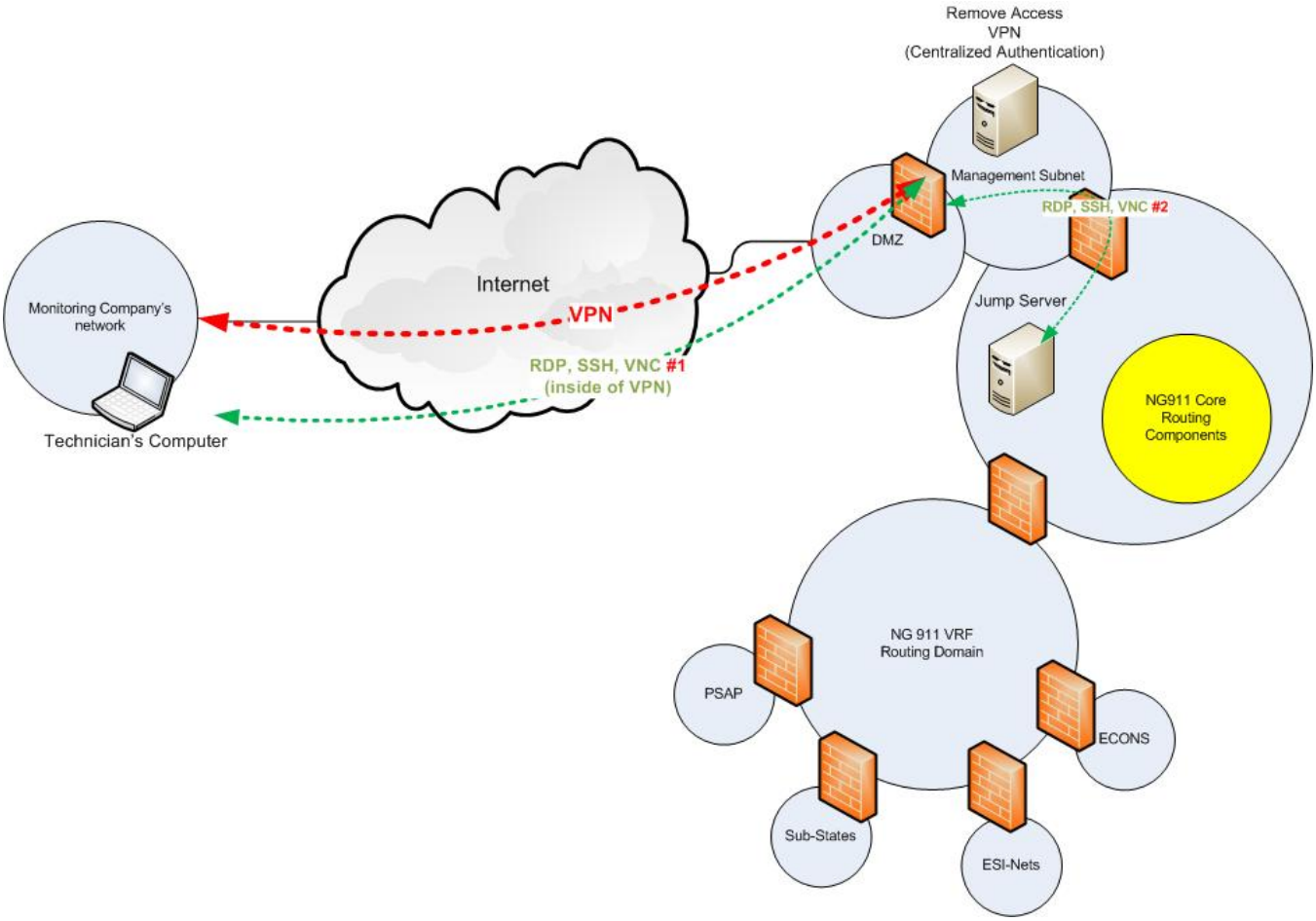


Figure 32—Jump Server

4.7.4.22 Remote access and removable devices such as USB drives for patches and laptops for maintenance shall be kept secured and scanned for malicious software and current configuration prior to joining the network. Any removable device must be inspected automatically by the system to verify the device is virus free prior to being authenticated by the system.

4.7.5 Service Level Agreements (SLAs)

4.7.5.1 NG-911 Routing Service SLA Overview

4.7.5.1.1 The NG-911 Routing Service must be a highly available and highly reliable service. The successful Respondent must agree to stringent performance and operational service level commitments. These commitments are based upon guaranteed response times and performance measurements as described within the SLAs, with associated Department credits for non-compliance. These SLAs do not vary the technical specifications for these services. The NG-911 Routing Service levels are designed to ensure that the required performance and delivery expectations are satisfied.

4.7.5.1.2 Unless otherwise specified or agreed to, all SLAs shall be applicable on a per incident basis. The SLAs shall become immediately effective and applicable to all portions of the NG-911 Routing Service deemed operational.

4.7.5.1.3 Should a trouble condition be experienced, or a service threshold exceeded that impacts service, a trouble ticket shall be opened by either an automated system, the NG-911 NOC, by the MyFloridaNet NOC, or by customer representatives. Once a trouble ticket has been issued by the NG-911 NOC, the successful Respondent, users, and MyFloridaNet representatives will work together to restore service outages and/or resolve service issues.

4.7.5.1.4 A trouble condition shall be classified as one of the following types:

- Critical Problem
- Major Problem
- Minor Problem

4.7.5.1.5 The remedy for an SLA violation will be based upon the classification of the trouble. Appropriate credits will be applied to the Department's account and will be capped at 100 percent of the successful Respondent's total monthly billing.

4.7.5.1.6 The successful Respondent, the Department, and customer representatives shall have the ability to monitor and verify NG-911 Routing Service SLA adherence via the NG-911 monitoring system and via access to the consolidated operational and transactional logs. The successful Respondent will not be held responsible for trouble conditions in the IP WAN services provided by MyFloridaNet that generate service issues that violate NG-911 Routing Service SLAs, nor for issues occurring on an external side (ECON, PSAP, other ESInet, etc.) of any demarcation, provided that the successful Respondent's own actions are faultless with respect to the required operation and monitoring of the NG-911 Routing Service.

4.7.5.1.7 The Department will meet with the successful Respondent on a monthly basis to review outage and performance degradation reports as part of managing these SLAs, including the assessment of penalties. Any applicable successful Respondent non-performance penalties shall be credited to the Department's monthly invoice.

4.7.5.2 Ingress and Egress Interconnection Types

4.7.5.2.1 For purposes of the SLAs, ingress and egress NG-911 Routing Service interconnections shall be classified as either reliable or unreliable interconnections. The choice of interconnection type lies with the interconnecting entity, and not with the successful Respondent. Therefore, the successful Respondent will be provided relief from certain SLA requirements for unreliable interconnections.

4.7.5.2.2 To be classified as reliable, an interconnection shall satisfy the following criteria:

- At least two geographically diverse physical (Layer 1) communications links each terminated to a successful Respondent-provided firewall, SBC, or gateway at geo-diverse locations.
- The call signaling formats utilized are in accordance with the specifications of the Florida NG-911 Routing Service.
- For ingress traffic, the interconnecting entity must support automatic failover at the application layer if a connection link fails or if the successful Respondent's equipment fails to return the expected signaling on that link within a short (less than five seconds) timeout interval. For egress traffic, the interconnecting entity must accept traffic on any link and cease to return handshakes, acknowledgements, or call progress signals if a downstream failure occurs in the interconnecting entity's link termination.

4.7.5.2.3 Interconnections that fail to satisfy the requirements of a reliable interconnection are classified as unreliable.

4.7.5.3 SLA Categories

4.7.5.3.1 Service levels are divided into the categories listed below.

- System-wide call processing (ingress to egress demarcations)
- Emergency call processing and delivery path components
- Auxiliary services
- Operational and notifications
- Security, Audits, and Reports

Exhibit H contains the SLAs in chart form.

4.7.5.4 System-wide Call Processing

The following SLAs deal concern the overall performance of the NG-911 Routing Service as it pertains to the processing and transport of emergency calls.

4.7.5.4.1 System Unavailability

This SLA is designed to assure that the system is available to process a 911 call 99.999 percent of the time, computed monthly.

Any total failure of any critical function (e.g., all instances of a reliable LNG fail or all instances of the ESRP fail) such that a call presented to that function during the failure interval would not be processed or forwarded to any destination, is a charge against System Unavailability. If the cumulative System Unavailability exceeds 30 seconds per calendar month, this SLA has been violated.

The system is deemed unavailable if it cannot deliver a call during an interval even if no calls actually arrive during the failure interval. If several instances of critical functions are not in service, yet a single instance of each critical function remains operational such that the system would still be able to deliver a call, then no charge against System Unavailability is made.

The Contractor can comply with this SLA by providing "soft fail" features in the system. For example, if all reliable LNGs are programmed with a default route such that if a total ESRP failure occurs, the LNG can still deliver a call to a default PSAP previously agreed upon by the Department, and this feature has been demonstrated and accepted by the Department, then a total ESRP failure does not start the System Unavailable clock. However, such a feature does not prevent the Contractor from quickly violating other SLAs, such as Emergency Call Delivery Accuracy, if the ESRP failure persists for any length of time.

The Department will monitor and analyze the NG-911 Routing Service component operational logs to determine if all instances of a critical process have failed concurrently. The log time-stamps will mark the beginning of the out-of-service interval for any instance of a critical process, and will mark the end of the interval when the process returns to service. Alternative tests, such as probes or test calls, may also be used to verify compliance with this SLA.

4.7.5.4.2 Ingress-to-Egress Call Delivery

This SLA is designed to assure that 99.999 percent of all calls actually received by the NG-911 Routing Service are delivered to an egress point such that they can be properly presented to a human operator. This SLA is a measure of system reliability rather than system availability. If more than 1 call per 100,000 received is not delivered anywhere, this SLA has been violated.

A call must actually have been received by the NG-911 Routing Service to count against this SLA. A call that was sent to the NG-911 Routing Service on an unreliable interconnection that is not operating does not violate this SLA. A call that is CANCELed before it can be delivered does not violate this SLA. On the other hand, delivering a call to an egress point that does not respond correctly does not constitute delivery. Only if the call is completely processed by the destination system is the call considered to have been delivered by the NG-911 Routing Service.

The Contractor can comply with this SLA by providing "roll-over" or "failover" routing in the PRF rulesets. If a destination does not respond within a timeout interval (which should be less than five seconds, unless ring-no-answer), the NG-911 Routing Service should present the call to an alternate destination in accordance with a plan previously accepted and demonstrated to the Department. However, excessive failovers due to a fault in the Contractor's system may result in other SLAs being quickly violated, such the Emergency Call Delivery Accuracy SLA.

The Department will monitor and analyze the NG-911 Routing Service transaction log database to verify that 99.999 percent of calls received by the NG-911 Routing Service were delivered to an egress interface.

4.7.5.4.3 Raw Logging Facility

Logging, required of all instances of critical functions in section 4.6.9, provides data utilized by the Contractor and the Department to demonstrate the proper operation of the NG-911 Routing Service. These logs may also become evidence in legal proceedings involving the handling of some particular emergency call. This SLA is designed to insure that required raw local data collection occurs.

The high-level design of the logging system as discussed in section 4.6.9 allows the logging system to fail softly. For example, if the consolidation process fails for a time, local raw data continues to be collected, and the consolidated logs can be updated once the consolidation process is repaired with no loss of data.

However, if no local raw log data is collected, then log entries may be missing, and the high availability and high reliability status of the system may be undetermined for some interval of time.

All processes that must keep local raw log files should be designed and implemented in such a way that if the process cannot write to the local raw log file, that process immediately (within 30 seconds of receiving a write to local raw log error) performs an automatic shutdown so that it does not continue to process unlogged transactions. Log write failures could occur for a number of reasons, such as disk full, disk failure, or loss of file write permissions.

Processes not able to create local log entries and which continue to process transactions for more than 30 seconds violate this SLA. Violations will be detected if the consolidated transaction database shows transactions to/from the offending process over an interval of time, yet the log entries from that process are missing in the consolidated transaction database.

4.7.5.4.4 Vulnerability to Single Point-of-failure

By design, a highly redundant system can experience failures within the system that have no noticeable impact on the service that the system renders. However, when operating with failures present, the system has reduced or lost redundancy, and is therefore vulnerable to a service effecting outage in the event of further failures. This SLA is intended to assure full redundancy is restored promptly to reduce and control the risk of a serious service affecting outage.

The Vulnerability clock starts any time a critical component within the core system losses all redundancy. The Contractor has four hours to restore (at least) some level redundancy to stop the Vulnerability clock. Failure to restore some level of redundancy within the hour interval is a violation of this SLA. Exceptions will be made for Force Majeure circumstances, such as a hurricane, fire, or flood.

This SLA does not cover dual connection to a single PSAP site, as the Vulnerability created by a loss of redundancy to a PSAP impacts a much smaller population than a Vulnerability with the potential to take down service state-wide.

Violations will be detected by inspection of the operational logs and/or the monitoring system “health” logs.

4.7.5.4.5 Emergency Call Delivery Accuracy

This SLA assures the correct internal functioning of the NG-911 Routing Service call routing functions, namely the SIP event server, the PRF, and the ECRF. These components calculate the “preferred” destination of a 911 call based on the caller’s location as reported in the call setup SIP messages (via SIP location conveyance) and referencing the GIS database and the appropriate policy ruleset. If the call is forwarded to the destination based on this data, this SLA is satisfied, even if the data is inaccurate or in error. Errors in the GIS database, or in the policy rules, or bad caller location data are not charged against this SLA.

This SLA is satisfied if 99.99 percent of the emergency calls are routed in accordance with the supplied data and database. Violations will be determined by periodic analysis of the consolidated transaction log database.

4.7.5.4.6 Call Information Delivery

This SLA assures the quality of the call as perceived by the telecommunicator.

a. Location Data Forwarded – Location data that was present when the call was setup is presented at the egress demarcation. This is determined by inspection of the transaction log database.
b. Standard Voice Quality – The voice channel from ingress to egress within the NG-911 Routing Service achieves a MOS score of 4.0 or better. This parameter is measured by probing and sampling the system near ingress and egress demarcations, or by an approved alternate measurement.
c. Useable Voice Quality – A minimum level of voice channel performance, unpleasant but intelligibility is not significantly impaired. Measured as in Standard Voice Quality, but MOS score must be 2 or greater.

This SLA requires 99 percent of all voice calls to satisfy criteria a) and b), and 99.9 percent of all calls to satisfy criteria c). The voice probe/sampling technique measures quality in the NG-911 Routing Service only, and does not account for deficiencies in the ECON network or at the PSAP or interconnecting entity. However, the Contractor is contractually obligated to assist these parties in any way possible to resolve their voice quality issues, such as make measurements and report findings, swapping out demarcation points for testing/comparison purpose, and lending advice.

4.7.5.4.7 Chronic Service Problems

This SLA amounts to an "escalation" clause on repeat problems by imposing an additional penalty if the same issues come up more than three times for Major violation or five times for Minor violations in the same calendar month. For issues limited to an individual hardware component, each hardware item is counted separately, but system-wide software issues manifesting the same problem may be counted each time it occurs regardless of the instance that failed.

4.7.5.5 Emergency Call Processing and Delivery Path Components

The following SLAs concern any system component, including circuits, servers, routers, multiplexers, or software functions provided by the Contractor, whether at the data center or at a PSAP site, that participate in the processing and delivery of emergency calls.

4.7.5.5.1 Demarc Termination (Unreliable Interconnections, section 4.7.5.2)

This SLA imposes a more stringent penalty on repair time violations on equipment or systems that terminate unreliable interconnections with other entities, because failures of such components have emergency call delivery service impacts. As long as a contractor completes repairs within the agreed upon time, there is no penalty to the NG-911 Routing Service Contractor, as the decision to utilize unreliable interconnections rests with the connecting entity.

In most instances, these types of connections would be used to connect to small, low traffic volume PSAP sites, where a failure would mean a few calls per day routed to an adjacent "overflow" PSAP. The service impact in this scenario should be more of an annoyance than life or properly threatening. Nevertheless, the Department requires prompt repair of components impacting service.

4.7.5.5.2 Unscheduled Downtime (Includes Reliable Interconnection Terminal Equipment, section 4.7.5.2)

This SLA imposes a requirement for the prompt repair of equipment, components, or processes in the 911 call path, but, which due to redundancy, is not service effecting. Since the specifications call for three data centers and full capacity with one data center out-of-service, most call path functions, except to the PSAP site, are likely to be in triplicate, and so a single failure would not have an impact on service or create a single point-of-failure Vulnerability. Therefore, this SLA permits more time for the repair and restoration of such a single failure. However, a second failure would likely create the single point-of-failure Vulnerability with its much more stringent SLA requirements.

Failures under this SLA should show up promptly on the monitoring system, and should also show up in the operational logs. Measurement will be by log inspection and monitoring system alarms.

4.7.5.5.3 System Updates/Patches

This SLA sets standards for the prompt application of patches or updates that remediate service impacting issues or even those that resolve annoyance issues. Except in extreme emergencies and depending on the nature of the problem to be resolved by the patch or update, the Department may require testing on the test environment before application of any patch or update.

Patches or updates that are not service impacting shall be included in the Patch/Update Report. The Department may wish to go slow on such updates to permit more testing time, field experience, and planning for the patch or update.

a. Operational Impact – Patches required to resolve serious operational or security issues may be required to undergo review by the change review process. Application should occur within 24 hours of approval.
b. Annoyance but Limited Impact – Patches required to resolve non-serious or annoyance issues shall undergo the review process and should be applied within seven days of approval.
c. Reports – The Contractor shall provide a monthly report on the current patch/update level of each major software/firmware component in the call path, the dates new patches and updates become available, the release notes or other descriptions of the issues the patch resolves, and the recommended install date for the patch or update. This report shall be completed by the end of the calendar month following the month of the report.

Compliance with this SLA shall be administered by the change review process.

4.7.5.6 Auxiliary Services

4.7.5.6.1 Monitoring of Critical Functions

This SLA covers the operation of the tools that monitor the critical functions in the NG-911 Routing Service emergency call path(s). If these tools are not operational, then the system is running “blind,” and the Contractor and Department lose the ability to detect and repair issues before they become service effecting.

For this reason the Department places critical importance upon the availability of the monitoring tools. This SLA is violated if the tools cannot monitor the critical functions of the NG-911 Routing Service for more than 30 minutes in any calendar month.

4.7.5.6.2 Log Processing

The Raw Logging SLA places very stringent requirements on the collection of primary log data, which can be stored locally for up to 30 days. However, the system will contain many local raw logs distributed among multiple locations, and the ability to use log data to verify the operation of the system or troubleshoot a problem is greatly impaired without the raw log consolidation functions and, in the case of the transaction logs, loading into the transaction log database.

This SLA permits the Contractor up to eight hours to repair a log consolidation issue.

4.7.5.6.3 LVF and Public Portals

The LVF and Portal permit the public and ECON operators to validate addresses for correct routing in the NG-911 Routing Service. These operations are usually performed in a batch or ad hoc basis, so high availability is not a strong requirement. Nevertheless, it is important that outside entities be able to access these resources regularly. This SLA requires the LVF and web portal to be available for all but eight hours per calendar month. Measurement can be via the monitoring systems.

4.7.5.7 Operational and Notifications

4.7.5.7.1 Monitoring System Problem Detection

The monitoring system must detect a change is status of any monitored component in the emergency call processing and delivery path in five minutes or less, and raise an alarm if appropriate. For monitored items not in the call delivery path, the monitoring system must detect and display a status change within 15 minutes.

This requirement can be measured by comparing the operational or transaction logs that should display the actual time a process halted or errored with the time the monitoring system raised a health alarm. The health alarm should be noted not less than 5 or 15 minutes after the last transaction entry or the last operational log entry (such as an error or shutdown entry).

4.7.5.7.2 Alarm to Trouble Ticket Interval

An automated system or a NOC employee shall create a trouble ticket within five minutes for a Critical or Major alarm, and within 20 minutes for all other alarms, assuming the alarm requires remedial action or a report. Measurement is by comparing trouble ticket creation time with the monitoring system alarm log.

4.7.5.7.3 Trouble Ticket to Dispatch Interval

If required by the nature of the trouble ticket and the NOC Operations Guide, the NOC shall either dispatch a technician for on-site work or have a technician access the trouble item remotely. For Critical or Major trouble tickets, dispatch or remote access must occur within 30 minutes of trouble ticket creation. For all other tickets, dispatch or remote access must occur within two hours.

4.7.5.7.4 Notifications

Predetermined Department personnel must be notified of Critical or Major problems within 15 minutes of trouble ticket creation. If notification is required for non-Critical or non-Major problems, notification shall be given within two hours. The NOC shall record time of notification in the trouble ticket system as required.

4.7.5.7.5 Database Updates

Updates received from authorized parties for the GIS or Policy databases shall be reviewed (as required) and either uploaded into the production system or returned to the sender with notification of exceptions that must be resolved before the updates can be processed. The data shall be uploaded or returned within two business days of receipt.

4.7.5.8 Security, Audits, and Reports

4.7.5.8.1 Unauthorized System Access Report

The Contractor must prepare and file with the Department a monthly report listing each unauthorized or failed login attempt by system and user name with timestamps. The report is due at the end of the month following the report.

4.7.5.8.2 Security Breach Response

If a security breach is detected or identified, the NOC must notify the Department according to the established procedure within 15 minutes of detection of the breach.

Within 24 hours of the breach, the NOC shall submit a written report indicating the nature of the breach, what damage was caused, if any, remediation taken, and other details as appropriate.

4.7.5.8.3 Malicious Activity Report

The NOC shall prepare a daily Malicious Activity report summarizing the date, time, types and frequencies of Malicious Activity observed, and actions taken. The Report is due no later than five business days after the date of the activity.

4.7.5.8.4 Physical Access Control

a. Intrusion Notification – Immediate notification of proper authorities in accordance with policy.
b. Final Report on Intrusion – Summary of incident with date, time, place, name of Intruder (if known), actions taken, and outcomes.
c. Intrusion Attempts Report – A monthly report similar to 7.5-30, but listing attempts to gain physical rather than login access. This report may be combined with the Unauthorized System Access report.

4.7.5.8.5 System Audits

a. Component Acceptance Testing/Annual Inspection – An annual site inspection report; first report due at system acceptance.
b. System-wide Acceptance Testing/Annual Inspection – An annual system functional and logical inspection report, reviewing required databases, documents, procedures, etc.
c. Penetration Test and Report – An annual security penetration test from the public Internet, the 911 VRF, and from sampled PSAP sites.
d. PSAP Testing and Report – PSAP site inspection and testing as needed.
e. Data Center/Host Audit and Report – A quarterly review of the data center sites covering physical security, environmental conditions (power, UPS batteries, fire suppression), general site and equipment conditions.
f. Compliance Audits and Review – Annual security audit.

Annual reports are due at the end of the second month after the close of the reporting period. The quarterly data center report is due at the end of the month following the site visit.

4.7.5.9 Service Levels

Service levels will be measured in terms of service outage or performance characteristics as defined below. Service credits based on restoral time are subsequently defined for each associated type: Critical, Major, and Minor.

4.7.5.9.1 Critical Problems

Restoration within twice the SLA time limit:	25% of MRC
Restoration within ten times the SLA time limit:	50% of MRC
Restoration after ten times the SLA time limit:	100% of MRC

For raw logging: if a process handles live emergency call traffic and required raw log entries are missing, the damages shall be 25% of MRC per incident.

4.7.5.9.2 Major Problems

Restoration within twice the SLA time limit:	10% of MRC
Restoration within ten times the SLA time limit:	20% of MRC
Restoration after ten times the SLA time limit:	40% of MRC

For emergency call delivery accuracy: for misrouting of up to 1 call per 1,000, 10% of the MRC shall apply; for misrouting up to 1 call per 100, 20% of MRC shall apply; and for misrouting more than 1 call per 100, 40% of the MRC shall apply. These damages would accrue, at most, once per month. Misroutes due to database errors, incorrect ECON data, or other information supplied by other than the successful Respondent shall be forgiven.

4.7.5.9.3 Minor Problems

Restoration within twice the SLA time limit:	5% of MRC
Restoration within ten times the SLA time limit:	10% of MRC
Restoration after ten times the SLA time limit:	15% of MRC

For standard voice quality: for quality problems greater than 1 call per 100, 5% of MRC shall apply; for problems greater than 1 call per 10, 10% of the MRC shall apply; and if no calls meet standard voice quality, 25% of the MRC shall apply, assessed monthly.

For useable voice quality: for quality problems greater than 1 call per 1,000, 5% of the MRC shall apply; for problem greater than 1 call per 100, 10% of the MRC shall apply; and for problems greater than 1 call per 10, 25% of the MRC shall apply.

4.7.5.9.4 SLA Violation Schedules

Liquidated damages for SLA violations will generally be based on the length of the outage measured from the beginning of the violation until service is restored and meets SLA metrics, on a schedule based on the problem type, unless otherwise explicitly stated. These schedules can be relaxed in any specific circumstance with the consent of the Department.

4.7.5.10 SLA Exclusions and Qualifications

Please note the following exclusions from service levels and credits:

- The successful Respondent is not responsible for the operation of MyFloridaNet, ECONs, PSAPs, or other interconnecting entities. The NG-911 Routing Service successful Respondent will not be charged for issues and problems originating among these entities provided the successful Respondent has properly coordinated maintenance and deployment activities with these stakeholders, and fully cooperates with problem resolution, even if the successful Respondent is not the root cause of the problem.
- Some SLAs may be excluded during scheduled maintenance periods with the prior arrangement and consent of the Department or authorized representatives.
- The successful Respondent is not responsible for circuits not purchased by the successful Respondent.
- The NG-911 Routing Service service levels will not be applicable due to Force Majeure. For example, delays directly due to acts of God, wars, acts of public enemies, strikes, fires, floods, or other similar cause wholly beyond the successful Respondent's control, or for any of the foregoing that affect subcontractors or suppliers if no alternate source of supply is available to the successful Respondent, other than what is specified in the COOP and recovery plan.
- Nothing in this section relieves the successful Respondent from complying with the specifications and requirements for the NG-911 Routing Service.

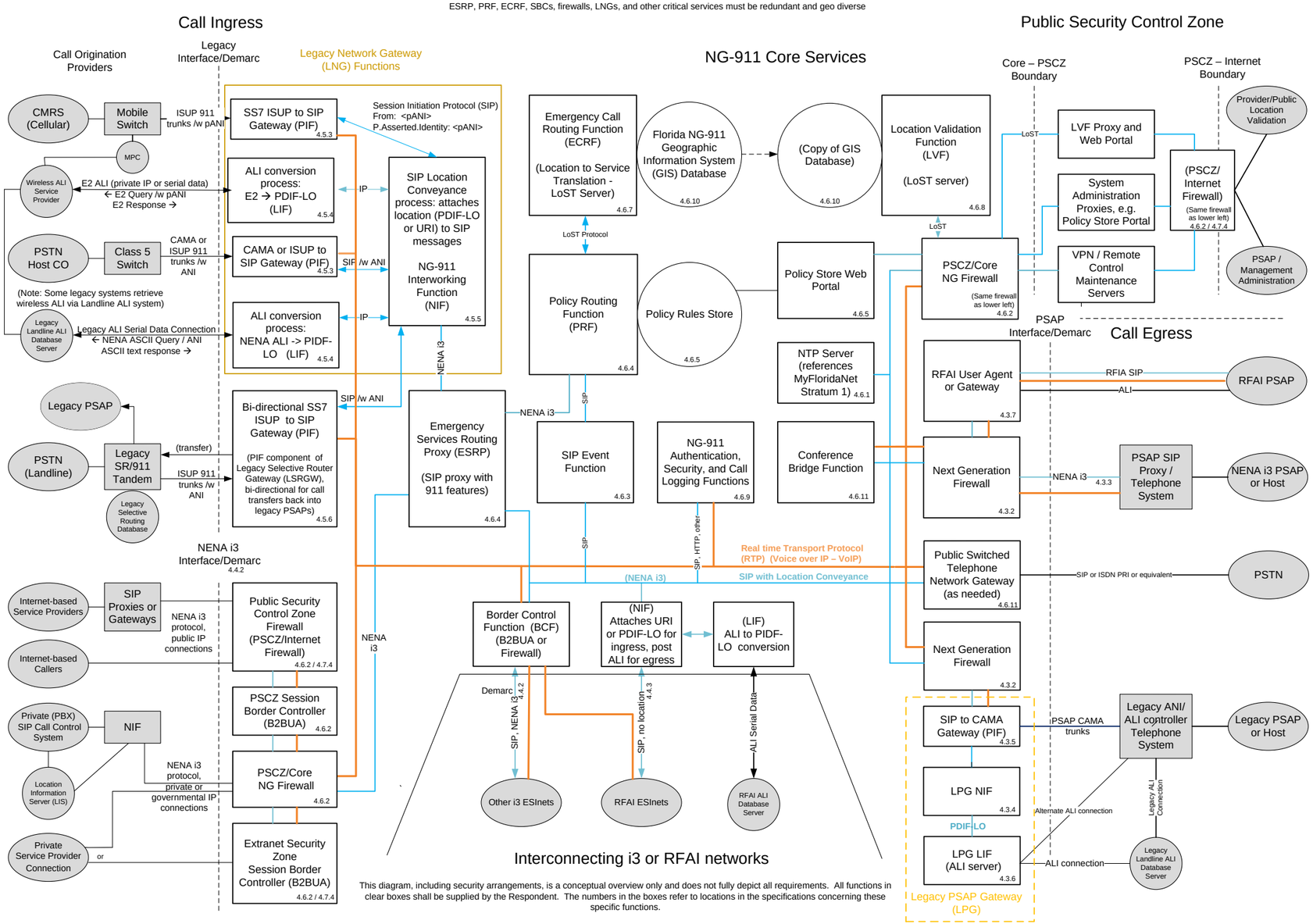
In addition to the requirements listed above, Respondents should highlight any distinguishing aspects of their service to be considered during the evaluation for the NG-911 Routing Service.

The remainder of this page is left blank.

Exhibit A—Conceptual Florida NG-911 Logical Diagram

SUNCOM NG-911 Routing Services Overview

ESRP, PRF, ECRF, SBCs, firewalls, LNGs, and other critical services must be redundant and geo diverse



This diagram, including security arrangements, is a conceptual overview only and does not fully depict all requirements. All functions in clear boxes shall be supplied by the Respondent. The numbers in the boxes refer to locations in the specifications concerning these specific functions.

Black lines are non-IP, or are on originating network side of demarc.

Blue lines IP signaling provisioned via NG-911 Service Provider private network or MFN ESInet VRF (4.2)

Orange lines IP media provisioned via NG-911 Service Provider private network or MFN ESInet VRF (4.2)

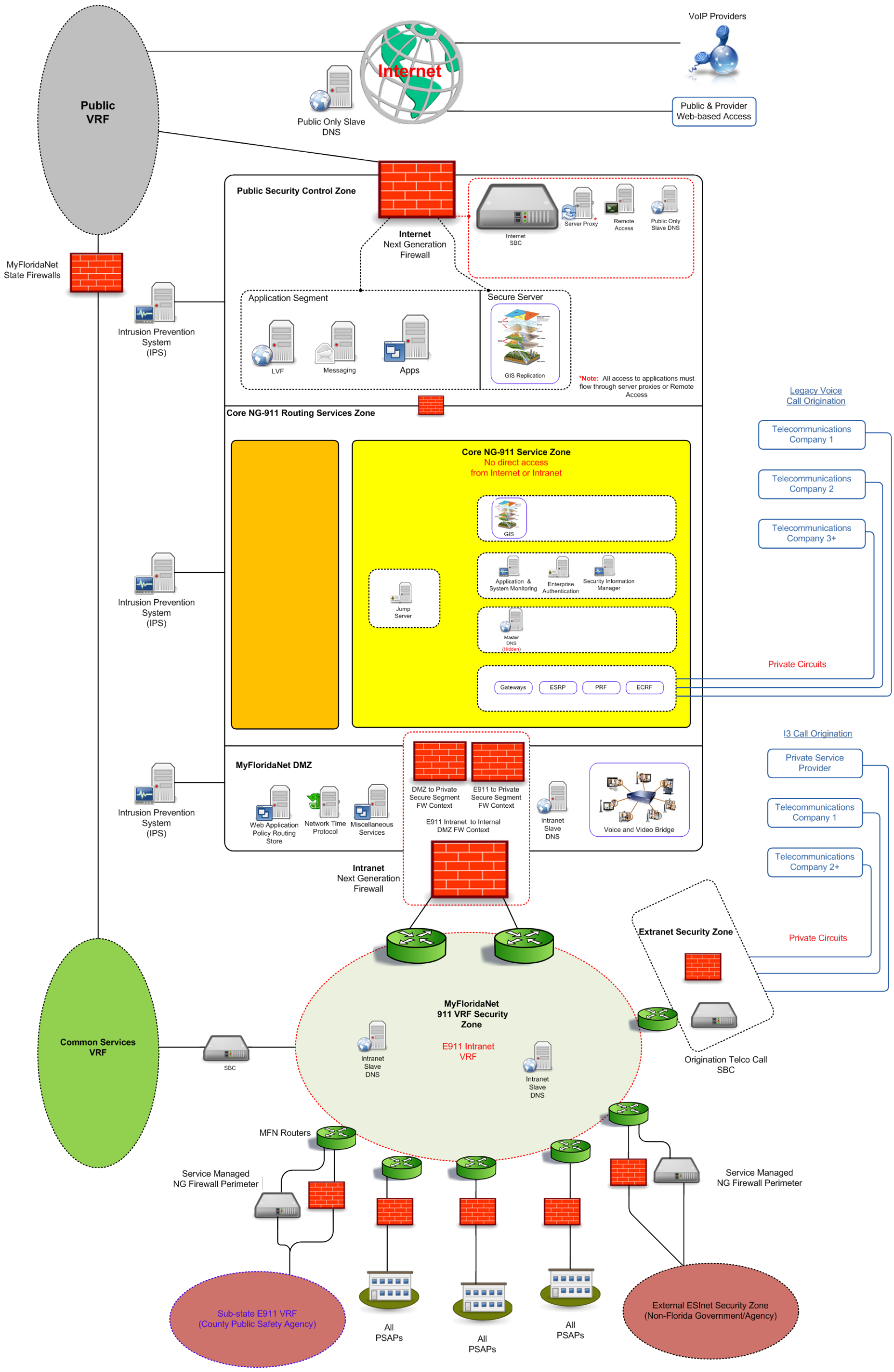
Return to Index

Exhibit B—Example of Security Zones

A sample security zone diagram may be found on the following page.

The remainder of this page is left blank.

NG-911 Routing Service Security Diagram



Return to Index

Exhibit C—Example Call Flows

Sample call flow diagrams may be found on the following pages.

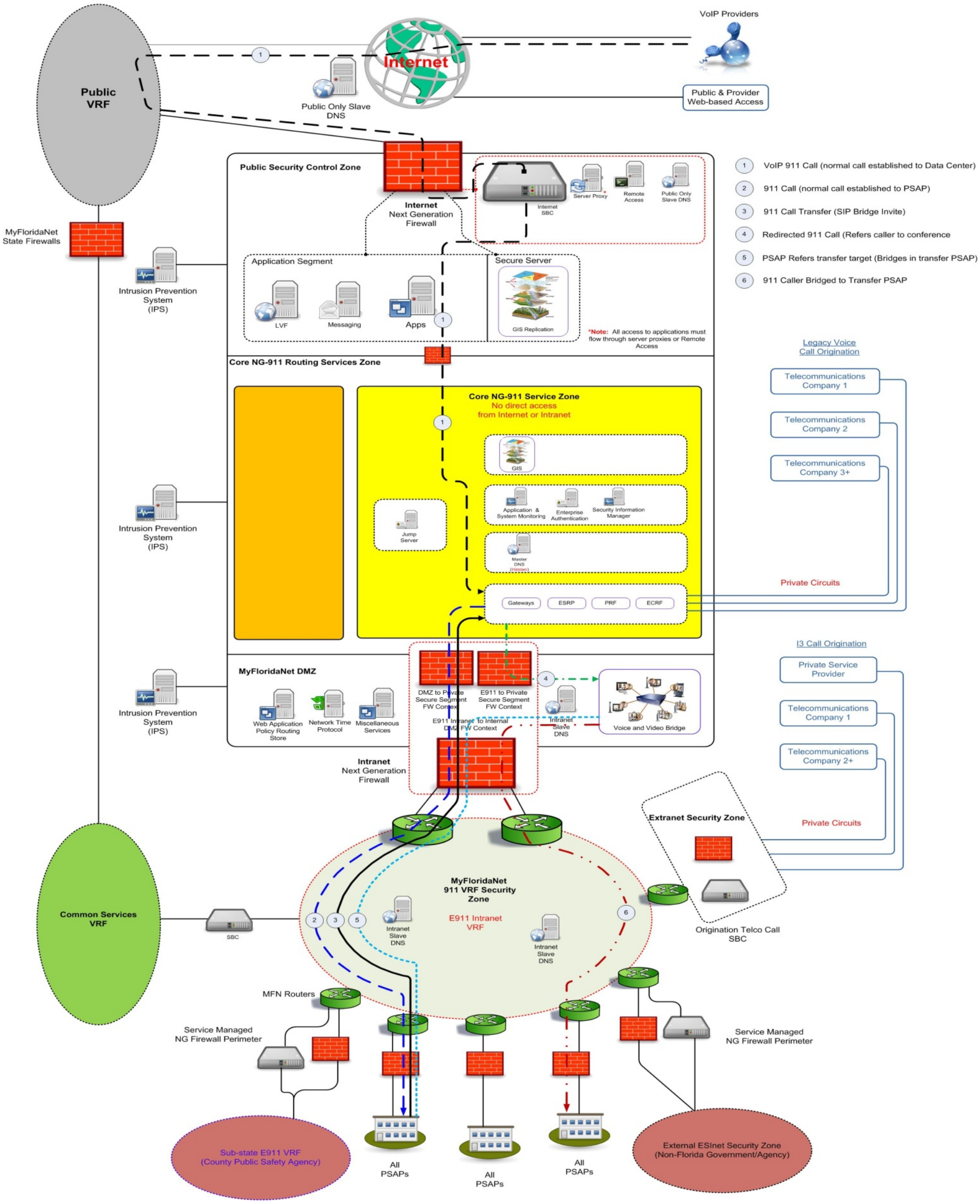
911 Call Flow and Process Control Security Zone Diagram Flow Descriptions

The NG-911 Routing Service is divided into distinct security zones. The network diagrams in this section provide diagrammatic conceptual network layouts for an understanding of how 911 calls and data flows through the NG-911 Routing Service security zone. Some process control is also depicted. The section does not include call flow diagrams detailing all the various wireline, wireless, and VoIP 911 call originations and terminations. The perimeter of each security zone is protected via next generation firewalls from the interconnected adjacent security zones. Refer to the security section for exact requirements.

The remainder of this page is left blank.

NG-911 Routing Service Security Diagram

(Security Strategy Diagram 1)



The remainder of this page is left blank.

VoIP Call Processing (Items #1 & #2)

Item #1 shows a VoIP 911 call being established to the Core NG-911 Routing Service and routed to the appropriate PSAP through Item #2. The VoIP provider provides the ingress of 911 emergency calls from the public Internet via NENA i3 signaling formats through the PSCZ next generation IPS firewall. The SIP call originating from the public Internet will terminate on one side of a SIP B2BUA SBC located within the PSCZ. The SBC re-originates the SIP call on the other side. The 911 call is processed through the next generation firewall at the Core NG-911 Routing Service security zone; this security zone observes the highest levels of security. The Core NG-911 Routing Service includes the Emergency Services Routing Proxy (ESRP), ECRF, and PRF for routing the 911 call. The 911 call is routed by the Core NG-911 Routing Service through the MyFloridaNet DMZ that interconnects the Core NG-911 Routing Service and the PSAPs. The 911 call is processed through the security zone next generation firewalls for delivery to the appropriate PSAP.

911 Call Transfer with Bridging Function (Items #3, #4, #5 & #6)

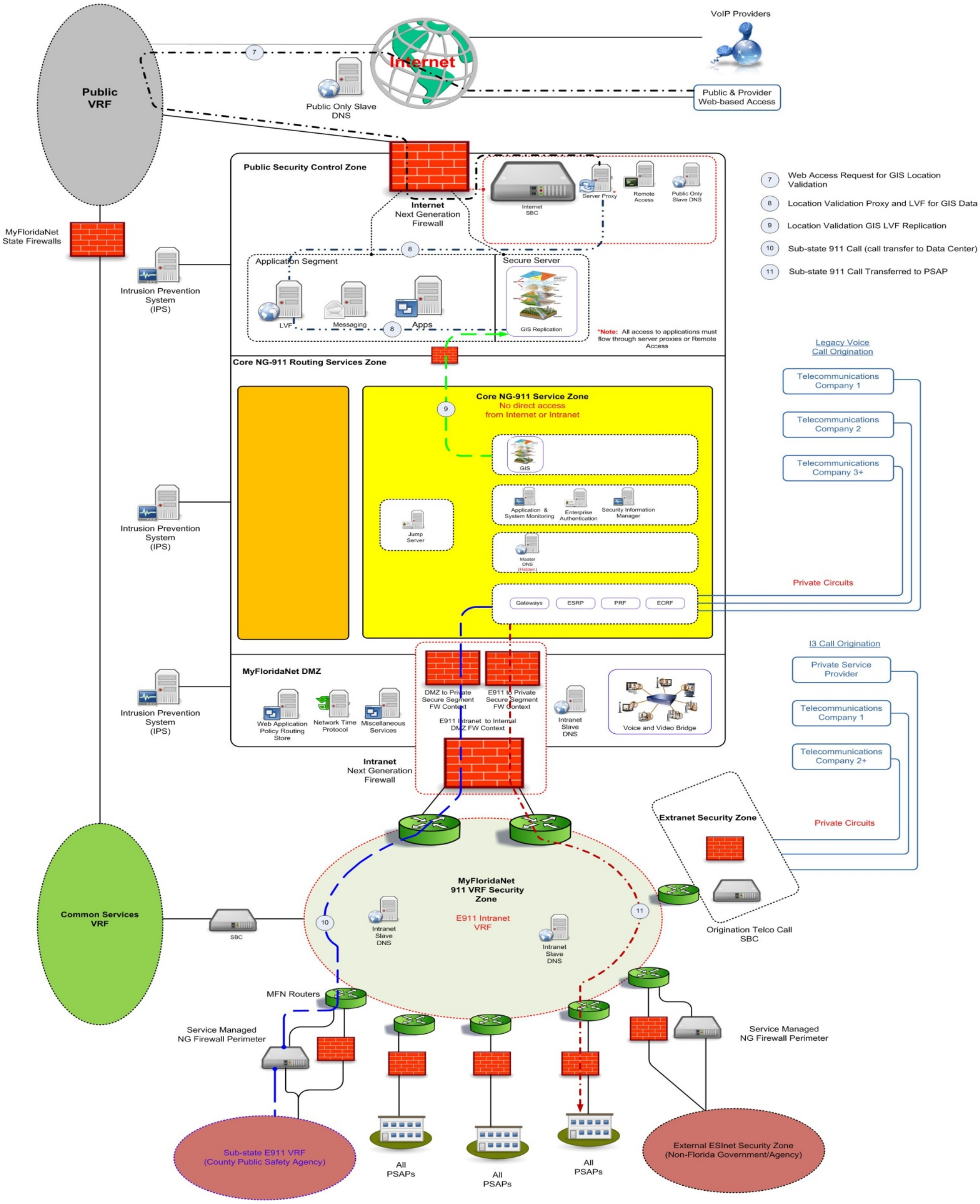
There are several scenarios for implementing 911 call transfers and conferences in an NG-911 system. In this scenario, bridging is performed through the NG-911 core bridging function. This bridging is used to transfer a 911 call and conduct a conference with another PSAP. The bridge has a SIP signaling interface to create and maintain conferences and multimedia capability (voice, video, text). This transfer sequence shows the PSAP transferring the 911 call using the MyFloridaNet IP infrastructure and the MyFloridaNet 911 VRF to the MyFloridaNet DMZ though next generation firewalls located at the PSAPs and the MyFloridaNet DMZ.

Item #3 shows the PSAP creating a conference on the bridge, which is located in MyFloridaNet DMZ; the PSAP refers the 911 caller to the bridge. The 911 caller's media path is moved to the bridge mid-call in Item #4 and the PSAP refers the target PSAP to the conference in Item #5. The transferred PSAP is then bridged on to the conference in Item #6.

The remainder of this page is left blank.

NG-911 Routing Service Security Diagram

(Security Strategy Diagram 2)



The remainder of this page is left blank.

Location Validation Function Access (Items #7, #8, & #9)

The public Internet may be used to obtain location status information about the NG-911 Routing Service. Citizens and ECON operators may utilize the public Internet to access LVF services. Item #7 shows an information request being established through the server proxy in Item #8 for the LVF application that has access to a replication of the ECRF GIS database. There is no direct access to the NG-911 Routing Service ECRF GIS database from the PSCZ. The NG-911 Routing Service provider is responsible for all changes to the ECRF GIS database and modifications are not made directly through the LVF. Item #9 shows the path for sending replication updates to the information in the LVF from the ECRF GIS database; these are provided through the PSCZ next generation firewall.

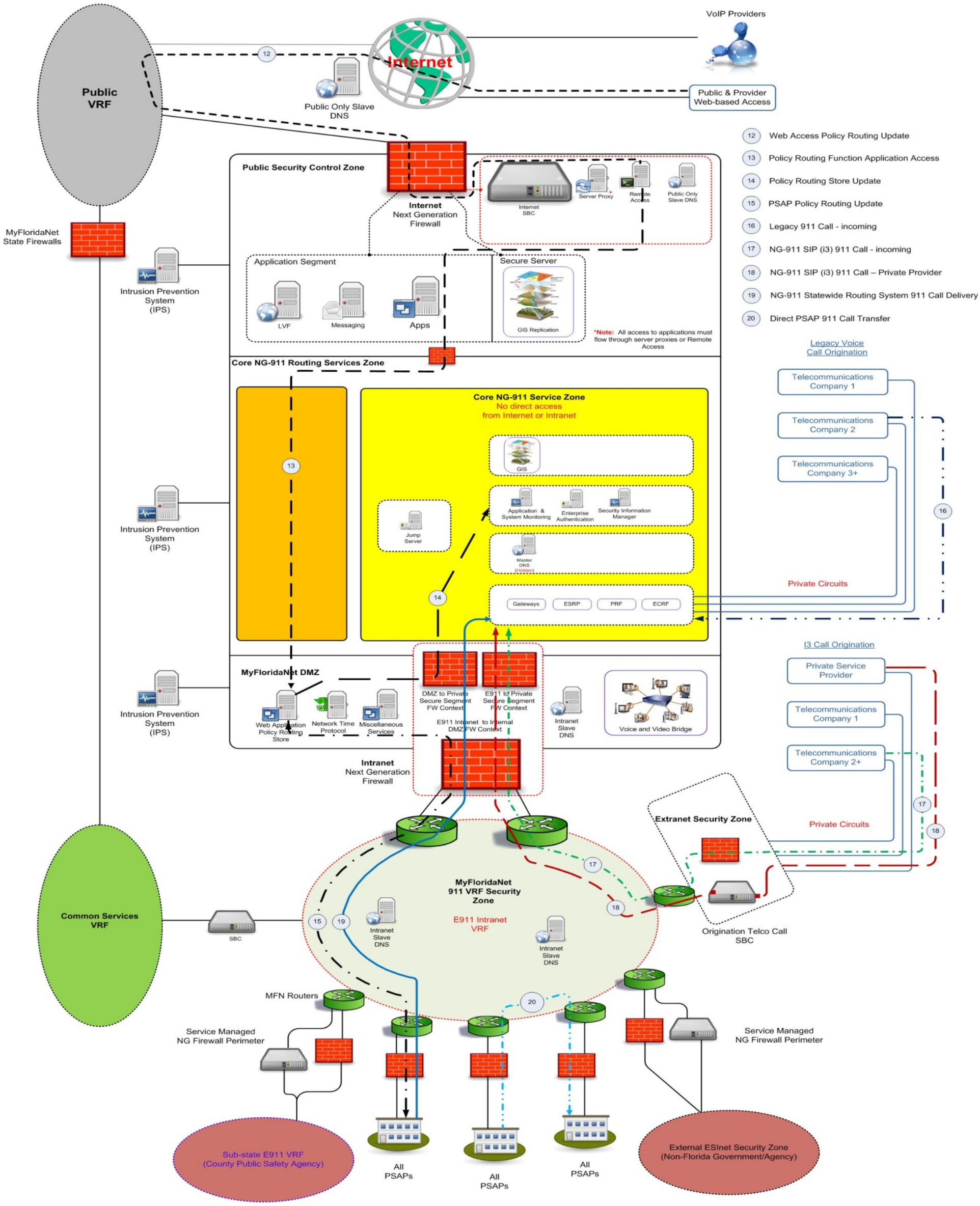
Sub-state 911 Call Transfer to System PSAP (Items #10 & #11)

These are existing Florida sub-state IP networks of PSAPs and other state ESInets that interconnect to the MyFloridaNet 911 VRF. These networks are interconnected via a next generation IPS firewall or an SBC as required by the NG-911 Routing Service. An SBC will depend on compatibility issues, such as use of IPv4 with the NG-911 Routing Service IPv6 core, or to resolve SIP signaling issues, such as non-support of the SIP "Replaces" header. Item #10 shows the transfer of a call through an SBC using the MyFloridaNet IP infrastructure and the MyFloridaNet 911 VRF through the MyFloridaNet DMZ next generation firewalls to the Core NG-911 Routing Service. The 911 call is routed in Item #11 by the Core NG-911 Routing Service back through the MyFloridaNet DMZ that interconnects the Core NG-911 Routing Service and the PSAPs.

The remainder of this page is left blank.

NG-911 Routing Service Security Diagram

(Security Strategy Diagram 3)



The remainder of this page is left blank.

Web Access Policy Routing (Items #12, #13, #14 & #15)

The public Internet may also be used for authorized personnel to remotely access the NG-911 Routing Service, including routing policy information required to support the delivery of emergency calls by the NG-911 Routing Service. Item #12 shows a routing access being established through the remote access application in the PSCZ through the next generation firewall. Item #13 shows the remote access application in the PSCZ through the next generation firewall through the Core NG-911 Routing Service security zone to the Routing Store Web application in the MyFloridaNet DMZ. Item #15 shows the county access to the NG-911 Routing Service at the PSAPs through the MyFloridaNet IP infrastructure and the MyFloridaNet 911 VRF through the MyFloridaNet DMZ next generation firewalls to the Routing Store Web application. The Web application has access to the Policy Routing Store in the Core NG-911 Routing Service in Item #14 through the Core NG-911 Routing Service next generation firewall.

Legacy 911 Call – Incoming (Item #16)

Legacy voice call originating carriers utilizing 911 analog trunks and existing databases will need to be processed through an LNG. Item #16 shows the connectivity to the LNG in the Core NG-911 Routing Service security zone.

NG-911 SIP (i3) 911 Call – Incoming (Item #17)

Telecommunications companies using their ECONs are interconnected to the MyFloridaNet 911 VRF for the purpose of delivering emergency calls to the NG-911 Routing Service in NENA i3 formats. When these networks are secure and considered trustworthy by the Florida NG-911 Routing Service, they are interconnected via the next generation firewall. Item #17 shows a 911 call processed through the MyFloridaNet IP infrastructure and the MyFloridaNet 911 VRF through the MyFloridaNet DMZ next generation firewalls to the Core NG-911 Routing Service.

NG-911 SIP (i3) 911 Call – Private Provider (Item #18)

There are private IP networks operated by ECONs that interconnect to the MyFloridaNet 911 VRF for the purpose of delivering emergency calls to the NG-911 Routing Service in NENA i3 formats. Item #18 shows the extranet security zone connection via a B2BUA SBC; this is separate from the PSCZ Internet SBC. This is required if the ECON's private IP network is incompatible with the Florida NG-911 Routing Service in some way, such as IP address space assignments or IPv4 vs. IPv6 issues, or to resolve SIP signaling issues. The 911 call is processed through the MyFloridaNet IP infrastructure and the MyFloridaNet 911 VRF through the MyFloridaNet DMZ next generation firewalls to the Core NG-911 Routing Service.

NG-911 Statewide Routing System 911 Call Delivery (Item #19)

The 911 call is routed by the Core NG-911 Routing Service through the MyFloridaNet DMZ that interconnects the Core NG-911 Routing Service and the PSAPs. The 911 call is processed through the security zone next generation firewalls for delivery to the appropriate PSAP.

Direct PSAP 911 Call Transfer (Item #20)

This scenario shows a PSAP implementing a 911 call transfer. In this scenario, bridging is performed through the PSAP equipment or bridge. Item #20 shows the PSAP transferring the 911 call using the MyFloridaNet IP infrastructure and the MyFloridaNet 911 VRF though next generation firewalls located at the PSAPs.

The remainder of this page is left blank.

Exhibit D—Current Call Volume Data

County	Number of Primary PSAPs	Number of Secondary PSAPs	Number of Back-up PSAPs	Number of 911 Calls/Year	County Population	Sub-State System
Alachua	1	0	1	153,778	247,337	
Baker	1	0	1	15,415	26,927	NFRS
Bay	2	6	0	132,790	169,278	
Bradford	1	0	1	17,390	28,662	NFRS
Brevard	10	1	0	341,191	545,184	AT&T
Broward	10	2	1	1,500,497	1,753,162	
Calhoun	1	0	0	4,404	14,685	Tri-County
Charlotte	2	0	1	73,694	160,463	Intrado IEN
Citrus	1	0	1	78,821	140,956	
Clay	3	1	0	91,428	191,143	NFRS
Collier	2	0	0	126,796	323,785	
Columbia	1	0	1	44,086	67,528	
DeSoto	1	0	1	9,546	34,708	
Dixie	1	0	1	6,945	16,385	NFRS
Duval	5	2	1	780,507	864,601	NFRS
Escambia	2	1	0	251,379	299,261	
Flagler	1	0	1	46,081	96,241	
Franklin	1	0	0	7,170	11,527	Tri-County
Gadsden	1	0	1	33,777	48,200	
Gilchrist	1	0	0	9,287	16,983	
Glades	1	0	1	24,021	12,812	
Gulf	1	1	1	6,186	15,789	Tri-County
Hamilton	1	0	1	10,546	14,744	
Hardee	1	0	1	10,254	27,653	
Hendry	4	0	0	16,367	38,908	
Hernando	1	0	1	77,799	173,078	
Highlands	1	0	1	127,120	98,712	
Hillsborough	7	2	1	831,565	1,238,951	
Holmes	1	0	1	7,050	19,901	
Indian River	1	2	1	108,208	138,694	
Jackson	1	1	0	39,066	49,964	
Jefferson	1	0	1	8,165	14,666	
Lafayette	1	0	0	5,786	8,752	NFRS
Lake	7	1	0	206,495	298,265	CenturyLink
Lee	4	1	1	410,730	625,310	

County	Number of Primary PSAPs	Number of Secondary PSAPs	Number of Back-up PSAPs	Number of 911 Calls/Year	County Population	Sub-State System
Leon	2	5	1	183,175	276,278	NFRS
Levy	1	0	1	24,153	40,767	Intrado IEN
Liberty	1	1	1	4,451	8,370	NFRS
Madison	1	0	0	15,286	19,298	NFRS
Manatee	2	2	1	228,907	325,905	
Marion	2	2	1	270,052	331,745	
Martin	2	1	1	116,132	146,689	Intrado IEN
Miami-Dade	7	0	1	3,175,050	2,516,515	
Monroe	2	1	0	59,016	72,670	
Nassau	1	1	1	79,385	73,684	
Okaloosa	3	6	1	117,530	181,679	CenturyLink
Okeechobee	2	0	0	42,071	39,870	
Orange	7	3	0	1,099,578	1,157,342	AT&T
Osceola	3	0	0	202,272	273,867	
Palm Beach	18	1	2	803,687	1,325,758	AT&T
Pasco	5	1	1	241,480	466,533	
Pinellas	1	10	1	530,063	918,496	
Polk	2	3	0	371,712	604,792	
Putnam	1	0	1	59,375	74,052	NFRS
Santa Rosa	2	2	0	64,445	154,901	
Sarasota	1	2	2	238,057	381,319	
Seminole	4	1	1	248,855	424,587	
St. Johns	2	0	1	78,566	192,852	NFRS
St. Lucie	1	0	1	332,181	279,696	Intrado IEN
Sumter	2	0	0	40,550	96,615	
Suwannee	1	0	0	26,950	43,215	NFRS
Taylor	1	0	1	14,202	22,500	NFRS
Union	1	0	1	6,510	15,473	
Volusia	3	2	0	313,635	495,400	
Wakulla	1	0	1	9,892	30,877	
Walton	1	2	0	32,904	55,450	CenturyLink
Washington	1	0	1	17,365	24,638	
Total	**165**	**67**	**46**	**14,661,827**	**18,905,048**	

Exhibit E—Staffing Worksheet

1. Please list time allocations for staff by functional description for amount of time allocated for the entire project as well as the FTE calculation by month and quarter in the table below.

Function	Rate	Total percentage of project hours allocated per month	FTEs per month	FTEs per quarter
Project Manager				
Subject Matter Expert: [insert title]				
[insert title, as needed]				
[insert title, as needed]				

Notes: These rates will be used for the duration of the project in determination of any price modifications/change requests. List any other positions included in Respondent Staffing Proposal but not enumerated here.

2. Please complete the following table describing your project management team.

Name	Role	Years of Experience in stated Role	Percent of Workweek dedicated to this Project - Initial	Percent of Workweek dedicated to this Project – Normal

3. Please complete the following table describing your project technical team.

Name	Role	Years of Experience in stated Role	Percent of Workweek dedicated to this Project - Initial	Percent of Workweek dedicated to this Project – Normal

4. Please submit resumes for each individual listed in the tables above.

Exhibit F—Sample Operations Guide

A sample Operations Guide may be found on the following pages.

The remainder of this page is left blank.

Exhibit G—Telephone Monitoring Tools Example

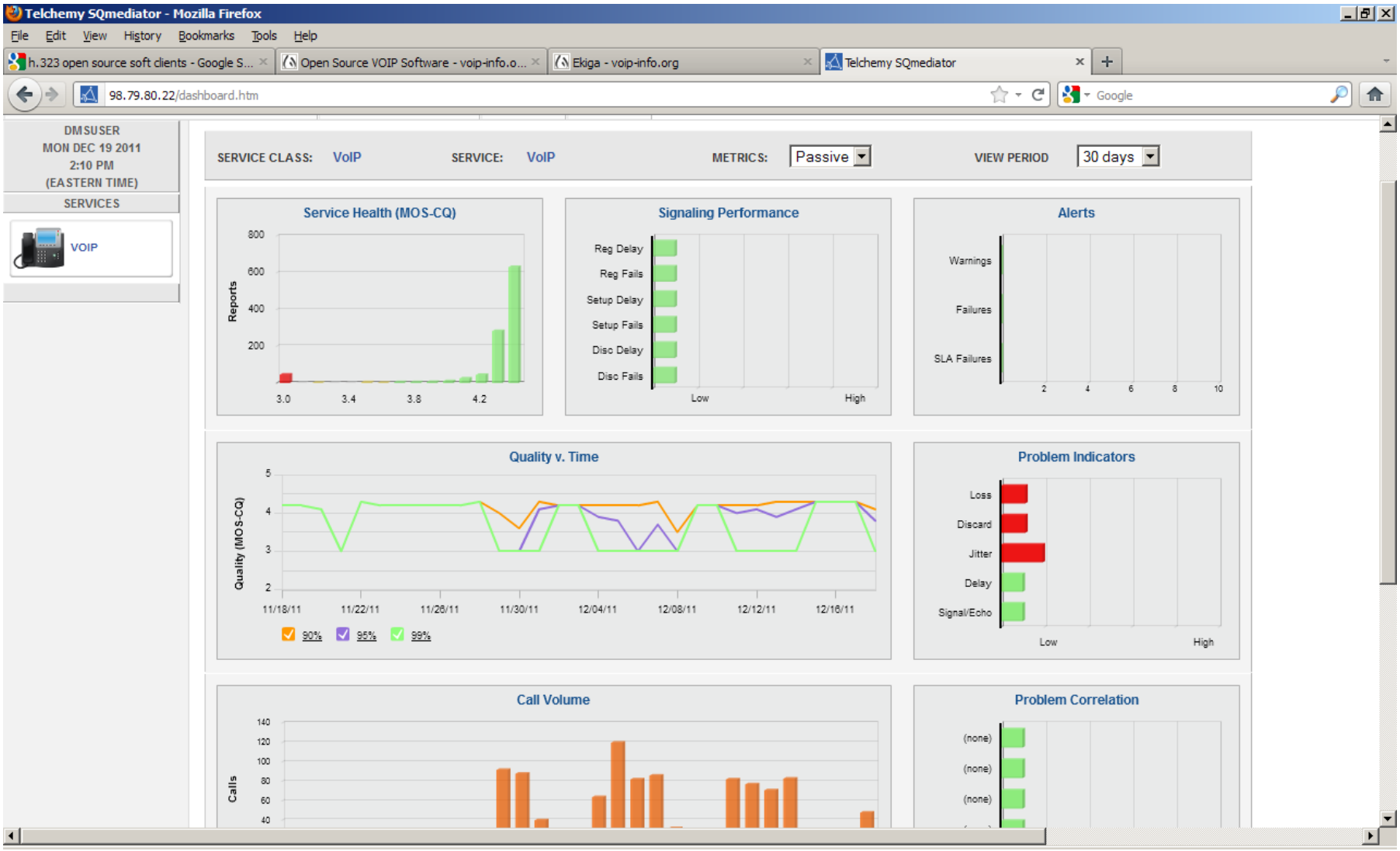
Enhanced 911 Technical Specifications

Telephony Measurement Tools and Reporting

Operational service tools and reports allow the Department and its customers to exercise oversight responsibility in the implementation, monitoring, troubleshooting, and adjusting of the NG-911 Routing Service functionality. The Department seeks functionality similar to that currently in use for MyFloridaNet hosted VoIP services.

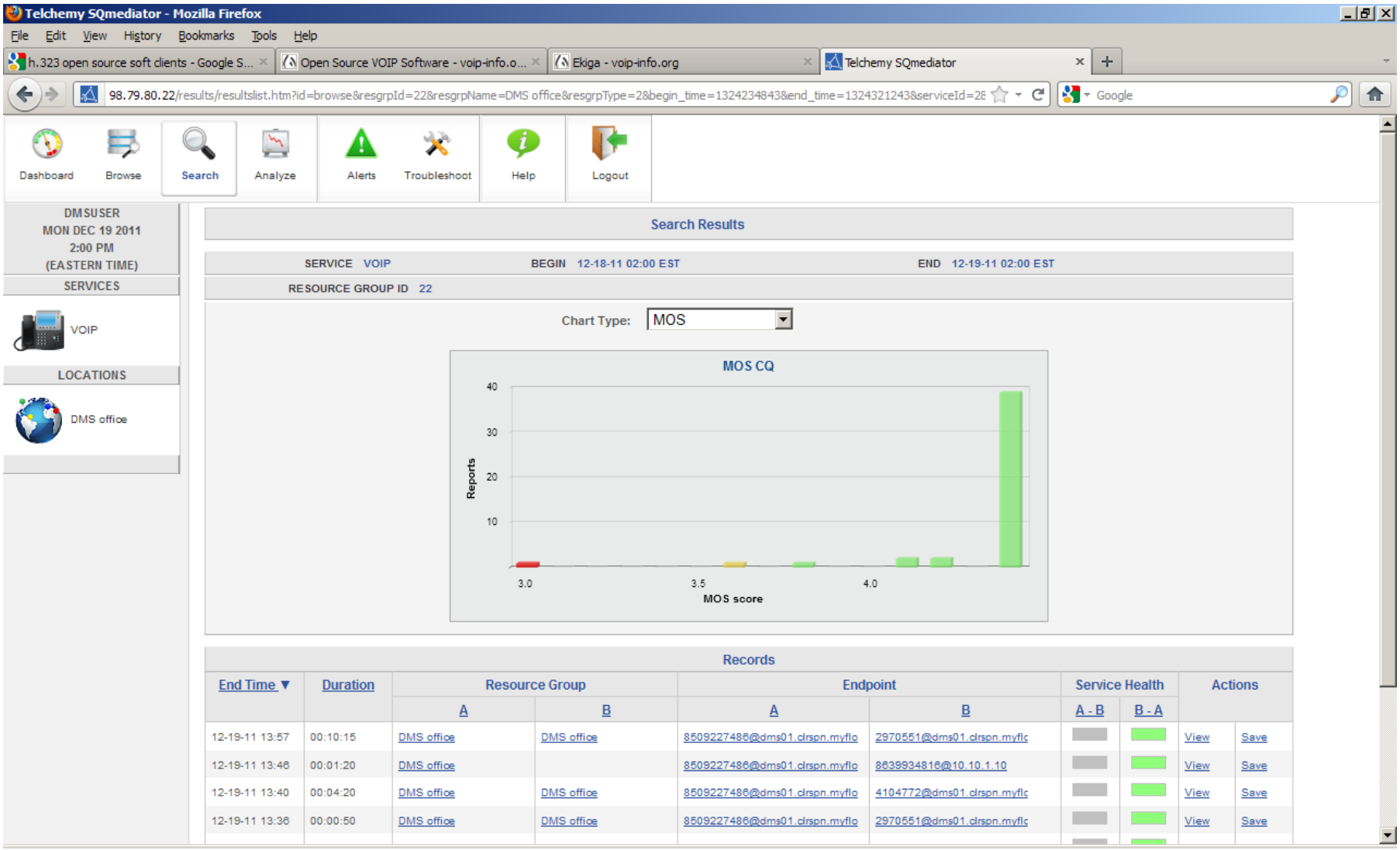
Functionally:

1. The Department plans to offer access to operational services to PSAP staff. Therefore access to all operational tools shall be web accessible using a standard web browser. Public Internet access from home 24x7x365 is required. Single sign-on for the entire suite of services is required. A common NG-911 theme is displayed.
2. A fundamental requirement of NG-911 telephony measurement tools is the ability to establish logical partitions that will be defined as dedicated views for specific PSAPs. The Department, NG-911 Routing Service customers, and Contractor management staff share management tools. The Department requires view/read-only access to the same parameters that the prime Contractor uses to manage the statewide NG-911 Routing Service. The Department requires a global view of tools, core equipment and services and any vendor-managed CPE. Telephony measurement tool views permit each PSAP to view their individual service domain. PSAPs are not able to view other PSAP domains unless authorized.
3. Retention time for measurements and monitoring output shall be one calendar year unless otherwise agreed.
4. Dashboard: All signaling and call quality shall be measured, reported and provided in a dashboard format.
    a. Overall service health
    b. Signaling performance
    c. Problem alerts and indicators
    d. Call volume
    e. Quantity vs. Time

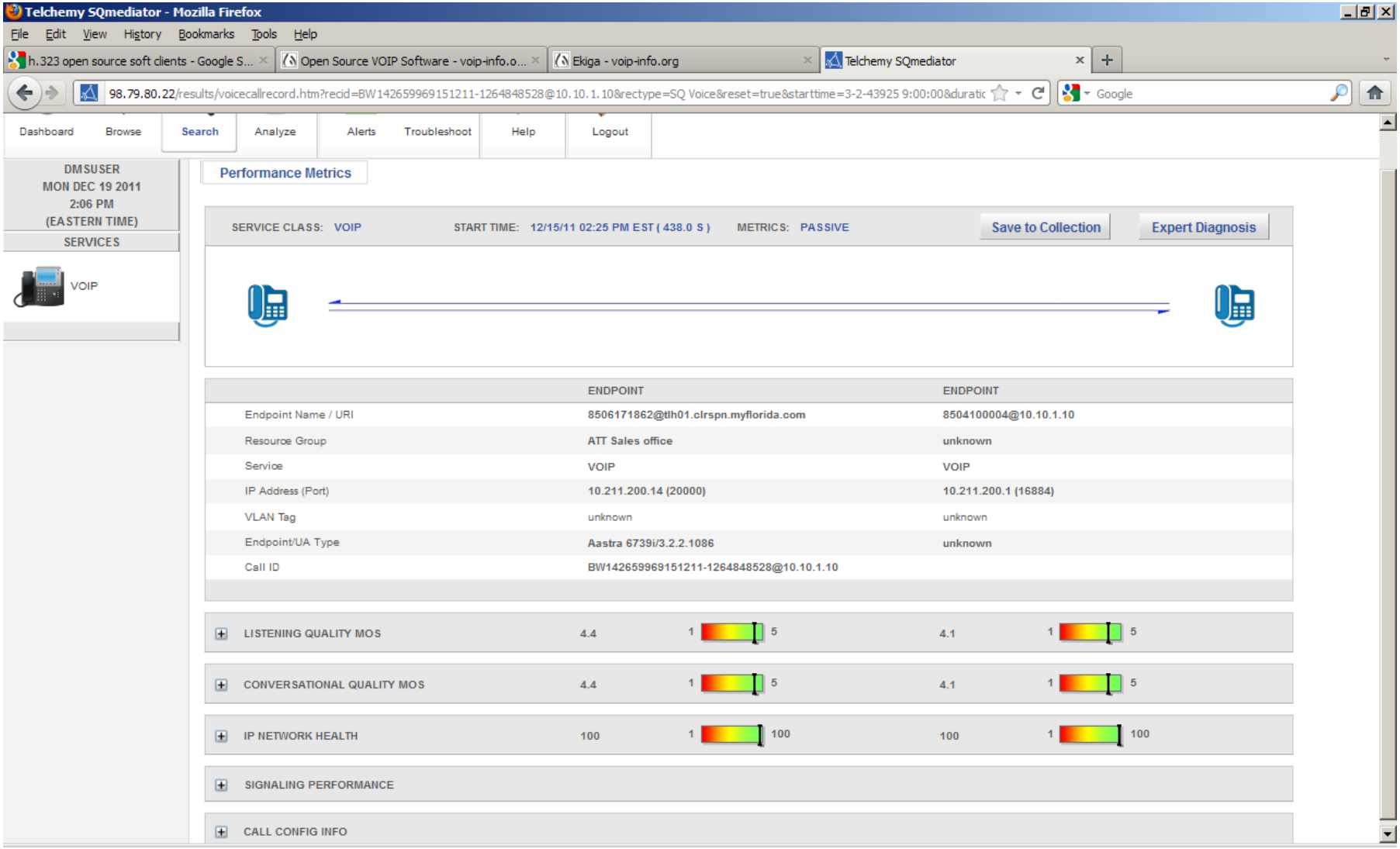


Return to Index

5. PSAP group summary: The tool shall be able to allow PSAP groups to display MOS call quality for all calls performed 24x7x365.

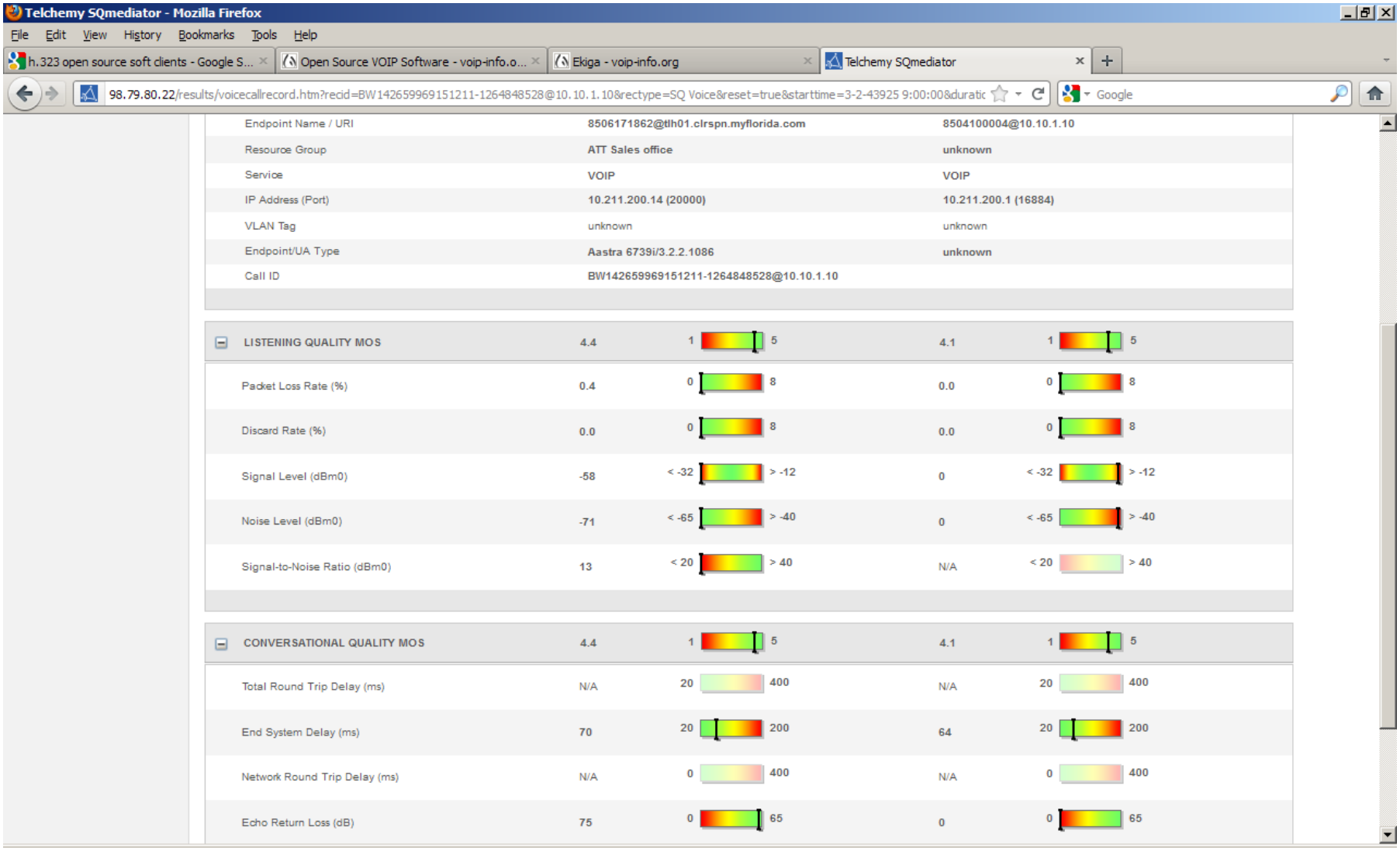


6. Specific call quality measurement summary view: The tool shall be able to report on specific calls for listening MOS, conversational quality MOS, IP network health, signaling performance, and anything related to a transferred call for 911.



Return to Index

7. Call quality measurement with listening and conversational MOS expanded:
    a. Listening Quality MOS: Packet loss rate, discard rate, signal level, noise level, and signal-to-noise ratio.
    b. Conversational Quality MOS: Total rout trip delay, end system delay, network round trip delay, and echo return loss.



8. Similar functionally to call quality with the expert diagnostics highlighted.

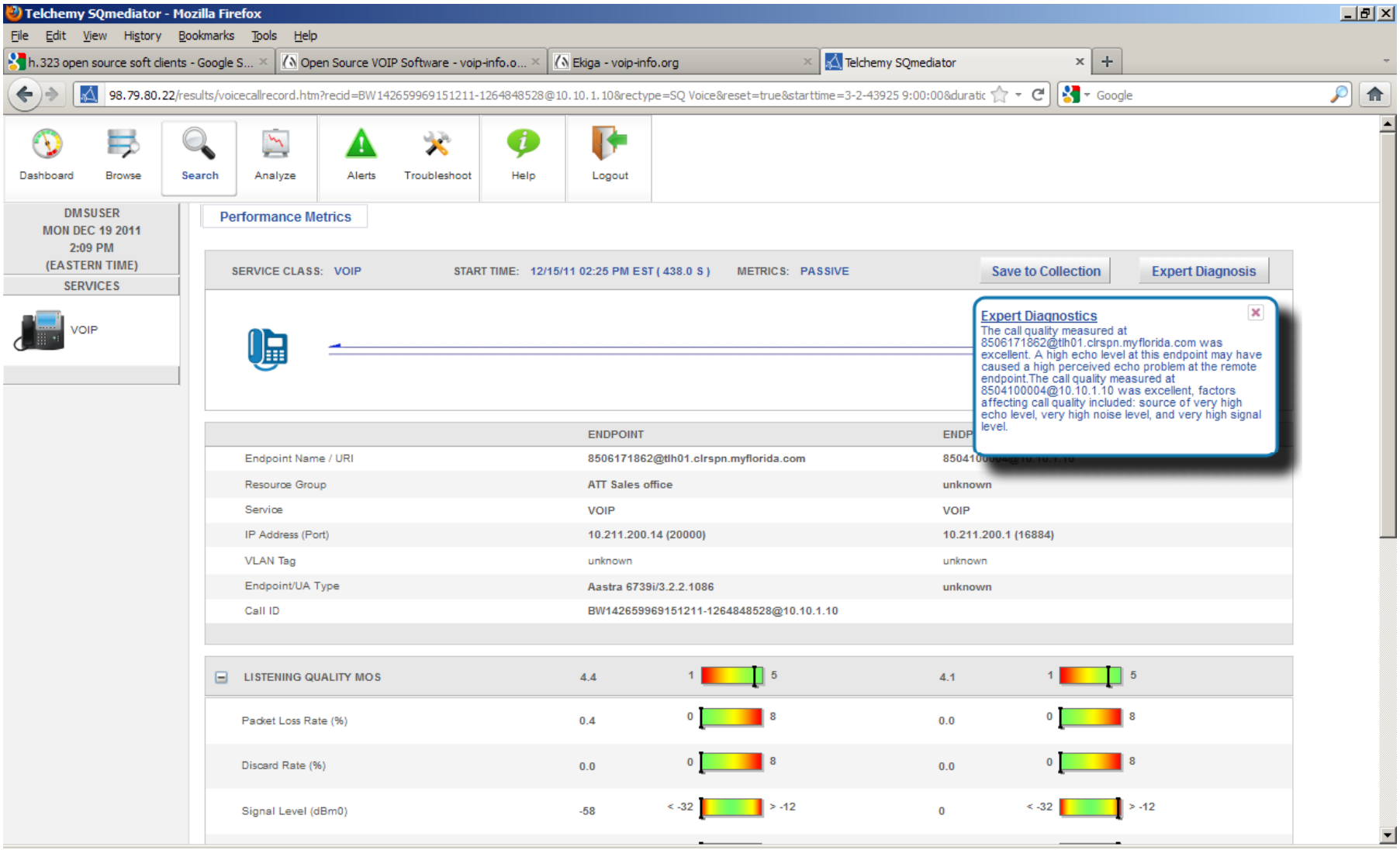


Exhibit H—Service Level Agreement Chart

SYSTEM WIDE CALL PROCESSING				
SLA	**Description**	**Measurement**	**Type**	**Penalty**
System Unavailability	Any failure of all instances of any critical function such as the ESRP, ECRF, or LNG, or infrastructure, which makes the NG-911 Routing Service unavailable for more than 30 seconds per month.	Software analysis of critical health alarms logs for each critical function instance.	Critical	Restoration within twice the SLA time limit: 25% of MRC Restoration within ten times the SLA time limit: 50% of MRC Restoration after ten times the SLA time limit: 100% of MRC
Ingress-to-egress Call Delivery Failure	Call delivery failure where a properly signaled call is received at an ingress demarcation and is not delivered to any egress demarcation.	By software analysis of the transaction log database for calls received and not canceled, but also not delivered to an egress point within 30 seconds.	Critical	Restoration within twice the SLA time limit: 25% of MRC Restoration within ten times the SLA time limit: 50% of MRC Restoration after ten times the SLA time limit: 100% of MRC
Raw Logging Facilities	Components and processes required to maintain local transaction and operational logs.	A component or process that is not able to create the "raw" (unprocessed) log entries and that is not shut down within 30 seconds.	Critical	If a process handled live emergency call traffic and required raw log entries are missing, the damages shall be 25% of the MRC per incident.
Vulnerability to Single Point(s)-of-failure	A failure creating critical single point(s)-of-failure in the surviving network, such that a subsequent failure of a surviving single point-of-failure would create a system unavailable situation.	By software analysis of health alarms, whereby a critical single point-of-failure exists for more than 4 hours. Exception for an "act of God" event that destroys a substantial portion of the system, e.g., hurricane floods a data center.	Major	Restoration within twice the SLA time limit: 10% of MRC Restoration within ten times the SLA time limit: 20% of MRC Restoration after ten times the SLA time limit: 40% of MRC

Emergency Call Delivery Accuracy	Emergency calls shall be delivered to the correct destination in accordance with the contents of the applicable databases and policies due to NG-911 Routing Service internal or functional issues.	Software analysis of transaction log database for calls arriving with correctly formatted location data, but where the final routing is due to default policies; also, based on PSAP trouble reports. Violation if error exceeds 0.01% of emergency call traffic in the calendar month.	Major	For misrouting of up to one call per 1,000: 10% of MRC For misrouting up to one call per 100: 20% of MRC For misrouting more than 1 call per 100: 40% MRC. These damages would accrue at most once per month. Misroutes due to database errors, incorrect ECON data, or other information supplied by other than the Contractor shall be forgiven.
Call Information Delivery Problems	Call traffic which is: Delivered without available data Delivered with below standard voice quality	Measured by voice quality monitoring tools and transaction log analysis. Violation if more than 5% of the total ingress-to-egress call traffic volume fails to meet the requirement for more than 5 minutes. This does not include calls received from external networks with missing data, or received at an ingress demarcation with below standard voice quality.	Major	Restoration within twice the SLA time limit: 10% of MRC Restoration within ten times the SLA time limit: 20% of MRC Restoration after ten times the SLA time limit: 40% of MRC
Standard Voice Quality	Standard voice quality obtains a Mean Opinion Score (MOS) of 4 or higher per ITU P.862E, and talker echo shall not exceed “acceptable” per ITU G.131. Includes all aspects of voice quality, including volume levels, dropouts, noise, etc.	Measured by automated voice quality measurement system. Violation if measurement fails to meet standards for more than 1% of the time over a calendar month. Exceptions for issues not under Contractor control, such as MyFloridaNet not in compliance with latency, jitter, and packet loss specifications.	Minor	Greater than 1% of measurements fail: 5% of MRC Greater than 10% of measurements fail: 10% of MRC All measurement fail: 25% of MRC Assessed monthly.

Useable Voice Quality	Useable voice quality obtains a MOS score of 2 or higher per ITU P.862E, and talker echo shall not exceed "limiting case" per ITU G.131. Includes all aspects of voice quality, including volume levels, dropouts, noise, etc.	Measured by automated voice quality measurement system. Violation if measurement fails to meet standards for more than 0.1% of the time over a calendar month. Exceptions for issues not under Contractor control, such as MyFloridaNet not in compliance with latency, jitter, and packet loss specifications.	Major	Greater than 0.1% measurements fail: 5% of MRC Greater than 1% of measurements fail: 10% of MRC Greater than 10% measurements fail: 25% of MRC
Chronic Service Problems	Repeated SLA violations of any category.	More than three occurrences of major SLA violation or more than five occurrences of minor SLA violation (concerning the same issue) in one calendar month.	Escalates subsequent violations one level.	Critical: Restoration within twice the SLA time limit: 25% of MRC Restoration within ten times the SLA time limit: 50% of MRC Restoration after ten times the SLA time limit: 100% of MRC Major: Restoration within twice the SLA time limit: 10% of MRC Restoration within ten times the SLA time limit: 20% of MRC Restoration after ten times the SLA time limit: 40% of MRC
COMPONENTS IN EMERGENCY CALL PATHS				
SLA	**Description**	**Measurement**	**Type**	**Penalty**
Demarcation terminal equipment and associated systems	Components whose failure interrupts unreliable interconnections, such as SBCs, LNG components, or firewalls.	Measured by inspection of device/process instance health logs. Violation if restoration exceeds 4 hours.	Major	Restoration within twice the SLA time limit: 10% of MRC Restoration within ten times the SLA time limit: 20% of MRC Restoration after ten times the SLA time limit: 40% of MRC

Unscheduled downtime	Unscheduled downtime each calendar month for any component or process instance in emergency call processing or delivery path that does not otherwise affect system operation.	Measured by inspection of device/ process instance health logs. Violation if unscheduled downtime exceeds 4 hours per month per device or process instance.	Minor	Restoration within twice the SLA time limit: 5% of MRC Restoration within ten times the SLA time limit: 10% of MRC Restoration after ten times the SLA time limit: 15% of MRC
Software/ firmware updates or patches	Software or firmware fixes required to repair identified deficiencies that impact some aspect of the operation of the service.	Repair within 2 weeks unless otherwise agreed. This does not relieve the Contractor from meeting all other SLAs.	Minor	Restoration within twice the SLA time limit: 5% of MRC Restoration within ten times the SLA time limit: 10% of MRC Restoration after ten times the SLA time limit: 15% of MRC
AUXILIARY SERVICES				
SLA	**Description**	**Measurement**	**Type**	**Penalty**
Critical monitoring functions	Tools that determine the current status of critical NG-911 Routing Service functions and components.	Violation if critical monitoring tools are unavailable for more than 30 minutes per calendar month.	Critical	Restoration within twice the SLA time limit: 25% of MRC Restoration within ten times the SLA time limit: 50% of MRC Restoration after ten times the SLA time limit: 100% of MRC
Log processing	Processes that produce consolidated logs and support log inspection.	Violation if consolidated logs are not updated for more than 8 hours. Exception if problem is due to WAN connectivity issues.	Major	Restoration within twice the SLA time limit: 10% of MRC Restoration within ten times the SLA time limit: 20% of MRC Restoration after ten times the SLA time limit: 40% of MRC

LVF and public portals	Processes and functions that permit the public to verify addresses or determine system status, etc.	Violation if public portals are unavailable for more than 8 hours per calendar month.	Minor	Restoration within twice the SLA time limit: 5% of MRC Restoration within ten times the SLA time limit: 10% of MRC Restoration after ten times the SLA time limit: 15% of MRC
OPERATIONAL AND NOTIFICATIONS				
SLA	**Description**	**Measurement**	**Type**	**Penalty**
Problem detection, monitoring system	Alarm must be raised that a device or process instance has failed or is out-of-service.	Analysis of combined operational log compared with monitoring system health logs. Violation if emergency call path failures are not alarmed within 5 minutes	Major	Restoration within twice the SLA time limit: 10% of MRC Restoration within ten times the SLA time limit: 20% of MRC Restoration after ten times the SLA time limit: 40% of MRC
		Violation if non-emergency call path failures are not alarmed within 15 minutes	Minor	Restoration within twice the SLA time limit: 5% of MRC Restoration within ten times the SLA time limit: 10% of MRC Restoration after ten times the SLA time limit: 15% of MRC
Alarm to trouble ticket entry	Create trouble ticket.	Critical or Major Alarms – Violation if trouble ticket not created within 5 minutes.	Major	Restoration within twice the SLA time limit: 10% of MRC Restoration within ten times the SLA time limit: 20% of MRC Restoration after ten times the SLA time limit: 40% of MRC
		Not Critical or Major Alarm – Violation if trouble ticket not created within 20 minutes.	Minor	Restoration within twice the SLA time limit: 5% of MRC Restoration within ten times the SLA time limit: 10% of MRC Restoration after ten times the SLA time limit: 15% of MRC

Trouble ticket entry to technician dispatch	Technician dispatched, or remote access initiated.	Critical or Major issues – Violation if dispatch time exceeds 30 minutes.	Major	Restoration within twice the SLA time limit: 10% of MRC Restoration within ten times the SLA time limit: 20% of MRC Restoration after ten times the SLA time limit: 40% of MRC
		Not Critical or Major – Violation if dispatch time exceeds 2 hours.	Minor	Restoration within twice the SLA time limit: 5% of MRC Restoration within ten times the SLA time limit: 10% of MRC Restoration after ten times the SLA time limit: 15% of MRC
Notifications	Notification of Department personnel of Critical or Major problem.	Violation if notification exceeds 15 minutes from time of trouble ticket.	Major	Restoration within twice the SLA time limit: 10% of MRC Restoration within ten times the SLA time limit: 20% of MRC Restoration after ten times the SLA time limit: 40% of MRC
	All other required notifications.	Violation if notification exceeds 2 hours from time of trouble ticket.	Minor	Restoration within twice the SLA time limit: 5% of MRC Restoration within ten times the SLA time limit: 10% of MRC Restoration after ten times the SLA time limit: 15% of MRC
Update databases	Policy or GIS database updates.	Updates must occur within 2 business days of update submittal.	Minor	Restoration within twice the SLA time limit: 5% of MRC Restoration within ten times the SLA time limit: 10% of MRC Restoration after ten times the SLA time limit: 15% of MRC
SECURITY				
SLA	**Description**	**Measurement**	**Type**	**Penalty**

Return to Index

Unauthorized system access	Report each invalid login attempt by users, including systems, attempting to access the network.	Report monthly. Violation if report not filed within following month.	Major	Restoration within twice the SLA time limit: 10% of MRC Restoration within ten times the SLA time limit: 20% of MRC Restoration after ten times the SLA time limit: 40% of MRC
Security breach	Immediate notification of a security breach.	Immediate telephone notification via established process. Violation if notification attempt not initiated within 15 minutes.	Critical	Restoration within twice the SLA time limit: 25% of MRC Restoration within ten times the SLA time limit: 50% of MRC Restoration after ten times the SLA time limit: 100% of MRC
	Final report.	Violation if report not submitted within 24 hours of resolution.		
Malicious activity	Reports from all system logs shall be combined to create a single report, which includes date, time, type of activity, response, and time to complete resolution.	Daily report. Violation if not submitted/available in the following 5 business days.	Major	Restoration within twice the SLA time limit: 10% of MRC Restoration within ten times the SLA time limit: 20% of MRC Restoration after ten times the SLA time limit: 40% of MRC
System updates and patches	System updates and patches to resolve issues with operational impacts.	Critical updates and patches to resolve issues seriously impacting system operation must be complete within 24 hours.	Critical	Restoration within twice the SLA time limit: 25% of MRC Restoration within ten times the SLA time limit: 50% of MRC Restoration after ten times the SLA time limit: 100% of MRC
		Updates and patches required to resolve annoying, but otherwise non-critical issues, must be installed within 7 days	Major	Restoration within twice the SLA time limit: 10% of MRC Restoration within ten times the SLA time limit: 20% of MRC Restoration after ten times the SLA time limit: 40% of MRC

	Report system update/ patch status: reason for update or patch; date update or patch became available; date implemented.	Monthly - Violation if report not completed in following month.	Minor	Restoration within twice the SLA time limit: 5% of MRC Restoration within ten times the SLA time limit: 10% of MRC Restoration after ten times the SLA time limit: 15% of MRC
Physical access control	Immediate notification of intruder.	Immediate telephone notification via established process. Violation if notification attempt not initiated within 15 minutes.	Critical	Restoration within twice the SLA time limit: 25% of MRC Restoration within ten times the SLA time limit: 50% of MRC Restoration after ten times the SLA time limit: 100% of MRC
	Final report.	Violation if report not submitted within 24 hours of resolution.	Major	Restoration within twice the SLA time limit: 10% of MRC Restoration within ten times the SLA time limit: 20% of MRC Restoration after ten times the SLA time limit: 40% of MRC
	Report outages, failed access attempts, other violations. Report shall include date, time, type of activity, response, and time to complete resolution.	Monthly - Violation if report not completed in following month.	Major	Restoration within twice the SLA time limit: 10% of MRC Restoration within ten times the SLA time limit: 20% of MRC Restoration after ten times the SLA time limit: 40% of MRC
System audits	Component acceptance testing; prior to implementation, thereafter annually.	Report upon completion of initial testing; thereafter include in a comprehensive annual report.	Minor	Restoration within twice the SLA time limit: 5% of MRC Restoration within ten times the SLA time limit: 10% of MRC Restoration after ten times the SLA time limit: 15% of MRC
	System-wide acceptance testing; prior to implementation, thereafter annually.	Report upon completion of initial testing; thereafter include in a comprehensive annual report.		

	Penetration testing from Internet, intranet, and extranet.	Annual report – Violation if not submitted within 2 months of test.		
	PSAP Testing.	Annual report – Violation if not submitted within 2 months of test.		
	Audit all hosts involved in 911.	Quarterly report – Violation if not submitted within 2 months of test.		
	Compliance audits and reviews.	Annual report – Violation if not submitted within 2 months of test.		

Exhibit I—List of Referenced Documents and Standards

MyFLoridaNet User Guide:
http://www.dms.myflorida.com/suncom/suncom_products_and_pricing/data_services/myfloridanet/mfn_resources/mfn_user_guide

ECRIT Standards: http://ecrit.sourceforge.net

ECRIT Implementation, http://ecrit.sourceforge.net

NENA i3 Technical Requirements Document. September 2006..
http://www.nena.org/standards/technical/voip/i3-requirements

NENA Functional and Interface Standards for Next Generation 9-1-1 (i3). December 2007.
http://www.nena.org/standards/technical/voip/functional-interface-NG911-i3

NENA Detailed Functional and Interface Standards for NENA (i3) Solution Stage 3 June 14, 2011.
http://www.nena.org/standards/technical/i3-solution

NENA GIS Data Collection and Maintenance Standards NENA 02-014, Issue 1, July 17, 2007.
http://www.nena.org/standards/technical/data/gis-data-collection-maintenance

NENA Master Glossary of 9-1-1 Terminology, NENA 00-001—Version 16, dated March 22, 2011,
http://www.nena.org/standards/master-glossary

Next Generation 9-1-1 (NG9-1-1) Architecture and Analysis Report. November 2007.
http://www.its.dot.gov/ng911/pdf/1.F2_FINAL_MED_ArchitectureAnalysis_v1.0.pdf

NRIC Best Practices
https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm

The Shortcut Guide to Improving IT Service Support through ITIL. Herold, Rebecca, 2007. Realtime Nexus.
http://nexus.realtimepublishers.com/sgitil.php

IETF Standards: www.ietf.org

IETF RFC 4346, The Transport Layer Security (TLS) Protocol, Version 1.1, April 2006
http://tools.ietf.org/html/rfc4346

IETF RFC 5491, GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations, March 2009 http://tools.ietf.org/html/rfc5491

IETF RFC 4119, A Presence-based GEOPRIV Location Object Format, December 2009
http://tools.ietf.org/html/rfc4119

IETF, RFC 5222, LoST: A Location-to-Service Translation Protocol, August 2008

Telcordia Standards
www.telcordia.com

TIA-942 Telecommunications Infrastructure Standards for Data Centers,
http://www.adc.com/Library/Literature/102264AE.pdf