Office of Emergency Communications (OEC) Interoperable Communications Technical Assistance Program (ICTAP)

Next Generation 911 (NG911) for Public Safety

Workshop for the State of New Jersey

January 23, 2015

Workshop Agenda

- Welcome & Introductions
- NG9-1-1 Technology
  - New Capabilities
  - ESInet
  - I3 Core Functions
  - Legacy PSAPs & an ESInet/i3
- Break — 15 mins
- PSAP Impacts
  - Operations
  - Capabilities
  - NG & GIS
  - Cybersecurity
  - Transition from Legacy to NG9-1-1
- Lunch on your own — 60 mins
- What Other States are doing
  - Massachusetts
  - Indiana
  - Tennessee
  - Mid-Atlantic Region
- Open discussion, Q/A

Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

OEC Technical Assistance Program

- The Department of Homeland Security (DHS) Office of Emergency Communications (OEC) partners with emergency communications personnel and government officials at all levels of government to lead the nationwide effort to improve national security/emergency preparedness communications capabilities
- OEC/ICTAP provides direct support to state, local, and tribal emergency responders and government officials through the development and delivery of training, tools, and onsite assistance to advance public safety interoperable communications capabilities

Presenters:	Email:
Joel McCamley, ENP	Jmccamley@yesinc.net
Nancy Dzoba	ndzoba@lafayettegroup.com

OEC Representatives:	Email:
Richard Tenney	Richard.Tenney@HQ.DHS.GOV
Christopher Tuttle	Christopher.Tuttle@dhs.gov

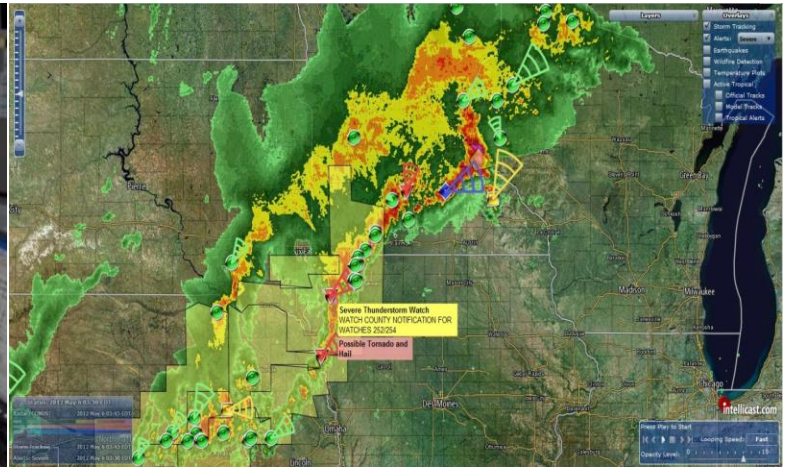
Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

NG911 Overview

- NG911 is an effort to enhance 911 capabilities by improving the hardware, software, and data and operational policies and procedures to:
  - Process various types of emergency calls including non-voice (multimedia) messages
  - Acquire and integrate additional data useful to call routing and handling
  - Deliver the calls/messages and data to the appropriate Public Safety Answering Points (PSAPs) and other appropriate emergency entities
  - Support data and communications needs for coordinated incident response and management
  - Address operational changes that will occur within the PSAP



Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

What is NG911?

- NG9-1-1 essentially refers to a fundamental change in the technology by which a 9-1-1 call for emergency service is routed to a Public Safety Answering Point (PSAP) and processed by the PSAP.

- It involves converting from analog based network technologies to digital or internet protocol (IP) based network technologies and in so doing allows for the transmission of more mission critical information related to the 9-1-1 call for emergency services.

- Examples include, pictures, videos, crash or telemetry data and real time location information of an emergency situation, with the overall goal to provide first responders with critical information so that a proper response can be achieved and the emergency situation resolved.

NG911 Improvements and Capabilities

Expand PSAPs and E911 Center capabilities

- Transfer voice and data between all NG911 PSAPs nationwide
- Directly activate alternate routing to control call volume
- Access a wide range of databases to expand data sharing and facilitate emergency response and comprehensive incident management

Enhance capability of current and new originating devices

- Non-voice messaging of various types
- Text-to-911
- Devices, such as sensors, generating data-only messages
- Photo and video transmission
- Telematics

Fully integrate and interoperate with other emergency systems and entities

- Other PSAPs
- Emergency Operations Centers
- DHS and other emergency management entities

Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

Community Expectations

- Same 911 access & service regardless of location, device
- High standards and requirements
- Reliable equipment & processes, esp. in disasters
- Warning notifications on social media, multimedia devices
- Equal access for special needs community

Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

NG9-1-1 Drivers in New Jersey

- Natural disasters like Sandy
- Large visitor population during peak times of year local, regional, national, international
- Proximity to other technology progressive urban areas like NYC and Philadelphia
- New Jersey's population, both in size and demographic
- Better public safety coordination facilitated by NG9-1-1 functions will improve response, and save lives

Additional NG911 Benefits

- Greater Responder Safety
  - Bio-Sensors (e.g., Building Sensors)
  - Gunshot Notification
  - Live Camera Monitoring
  - Transportation Ops Systems
- Enhanced Life & Property Protection
  - Advanced Roadway Technology
  - Smart Buildings
  - Vehicle Telematics
- Improved Interoperability
  - Call Transfer
  - Live Mapping
  - Mutual Aid Communications
- Accelerated Response Times
  - Geo-Location Information
  - Building Sensors
  - Real-Time Public Notification
  - Traffic Signal Pre-emption

NG911 Myths and Truths

- There are several myths and misconceptions encountered when discussing NG911—
  - The PSAP working environment will change radically overnight
  - Accurate location data is guaranteed
  - NG911 will immediately begin to save money
  - Harassing or malicious 911 calls will be eliminated

- Instead, NG911 is—
  - Migrating 911 from Legacy Circuit-Switched Technology to IP solutions
  - Establishing interconnected broadband networks for the processing and routing of calls for service and information exchange between agencies
  - Embedding location data in each call for service (No need to query databases)
  - Implementing dynamic management of call routing policy (operator loading, time-of-day, malfunctions, etc.)
  - Modernizing PSAP CPE (as needed)

Biggest Obstacles to NG9-1-1

Funding

Funding is the primary reason NG9-1-1 activity varies across the country. This can be complicated by a lack of understanding the need for change, lack of ability to 'save' or bank funds for future capital costs in budget requests, collected 9-1-1 fees used to pay for things other than 9-1-1 costs, are examples of where funding can become a challenge when considering the migration to NG9-1-1.

Lack of authority at state level agency

Only 35 states have an authorized and staffed public safety function related to 9-1-1.

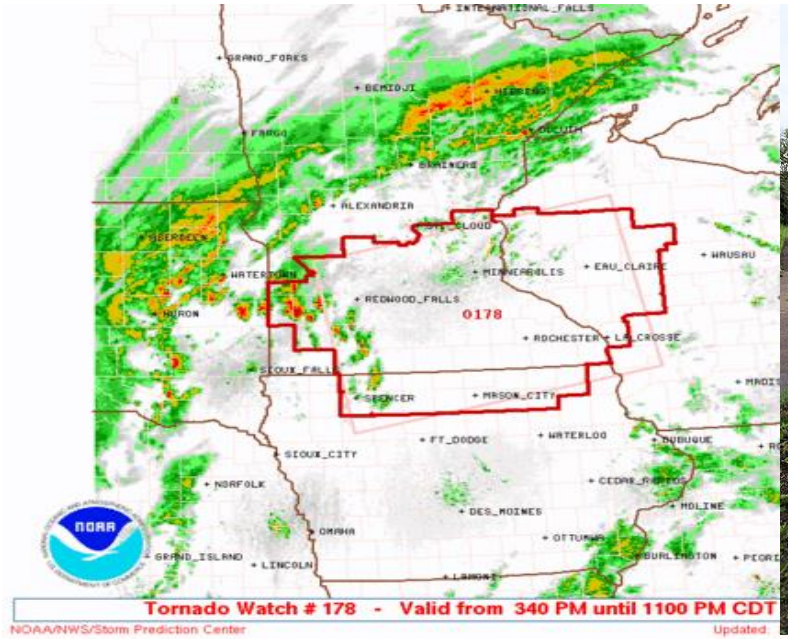
Legislation

Language specific to the way 9-1-1 was done in the past exists in many state statues that enable, regulate and require 9-1-1 service. In some instances, the language is so specific so as to exclude new service providers or alternative forms of technology that are necessary for the operation of 9-1-1 in a NG environment.

Contractual obligations

Some states are bound by existing, long standing contractual obligations based on old technology and how things used to be. The cost of terminating these types of contracts can be prohibitive and have prevented some jurisdictions from doing anything other than planning.

NG9-1-1 Technology



Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

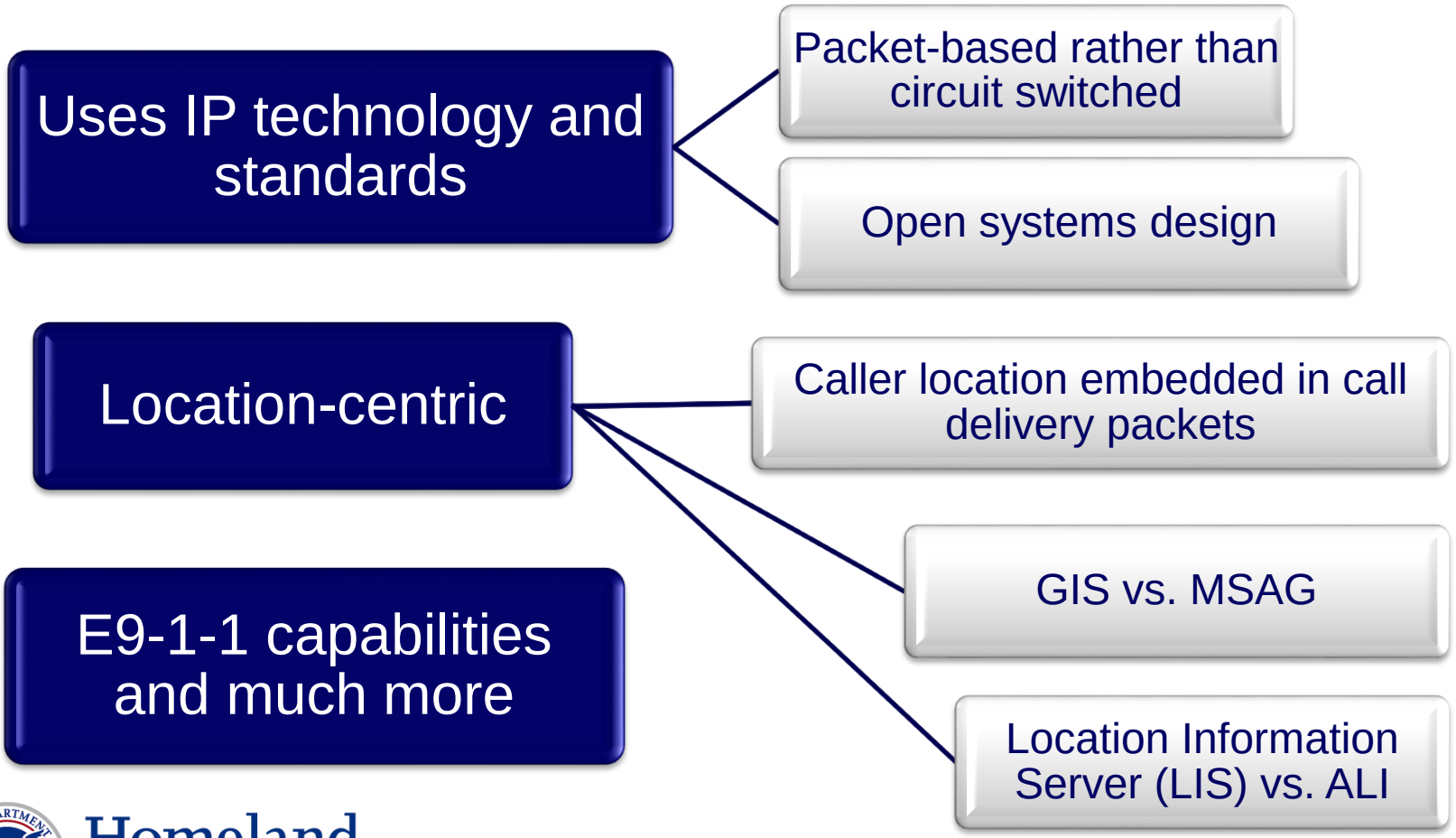
NG9-1-1 Technology: Definition

The set of network elements, software applications, databases, customer premise equipment (CPE) and operations and management procedures required to provide Next Generation emergency services

Includes the emergency services IP network and its interfaces defined in the NENA i3 standard

Includes elements outside the i3 standard including PSAP CPE, applications and operations

NG9-1-1 Technology: Differences



Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

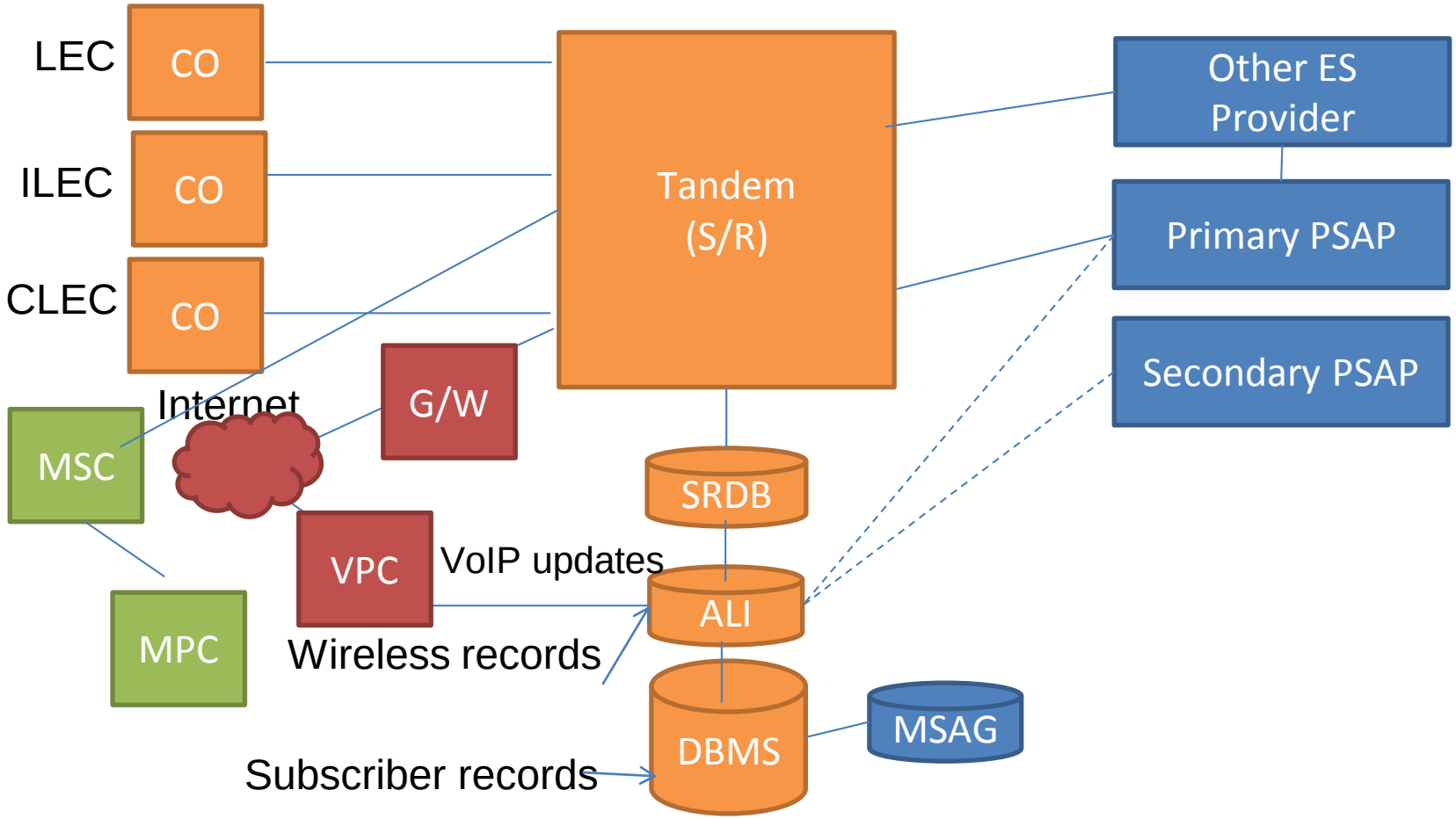
NENA i3 Standard and ESInet

The i3 Standard defines the Emergency Services IP Network (ESInet) and its interfaces

The ESInet is the IP transport infrastructure upon which independent application platforms and core functional processes can be deployed

In order to deploy a fully operational system, specifications of technical, operational, and human elements not covered in the i3 Standard are required

How 911 Works Typically Works Today



Homeland Security

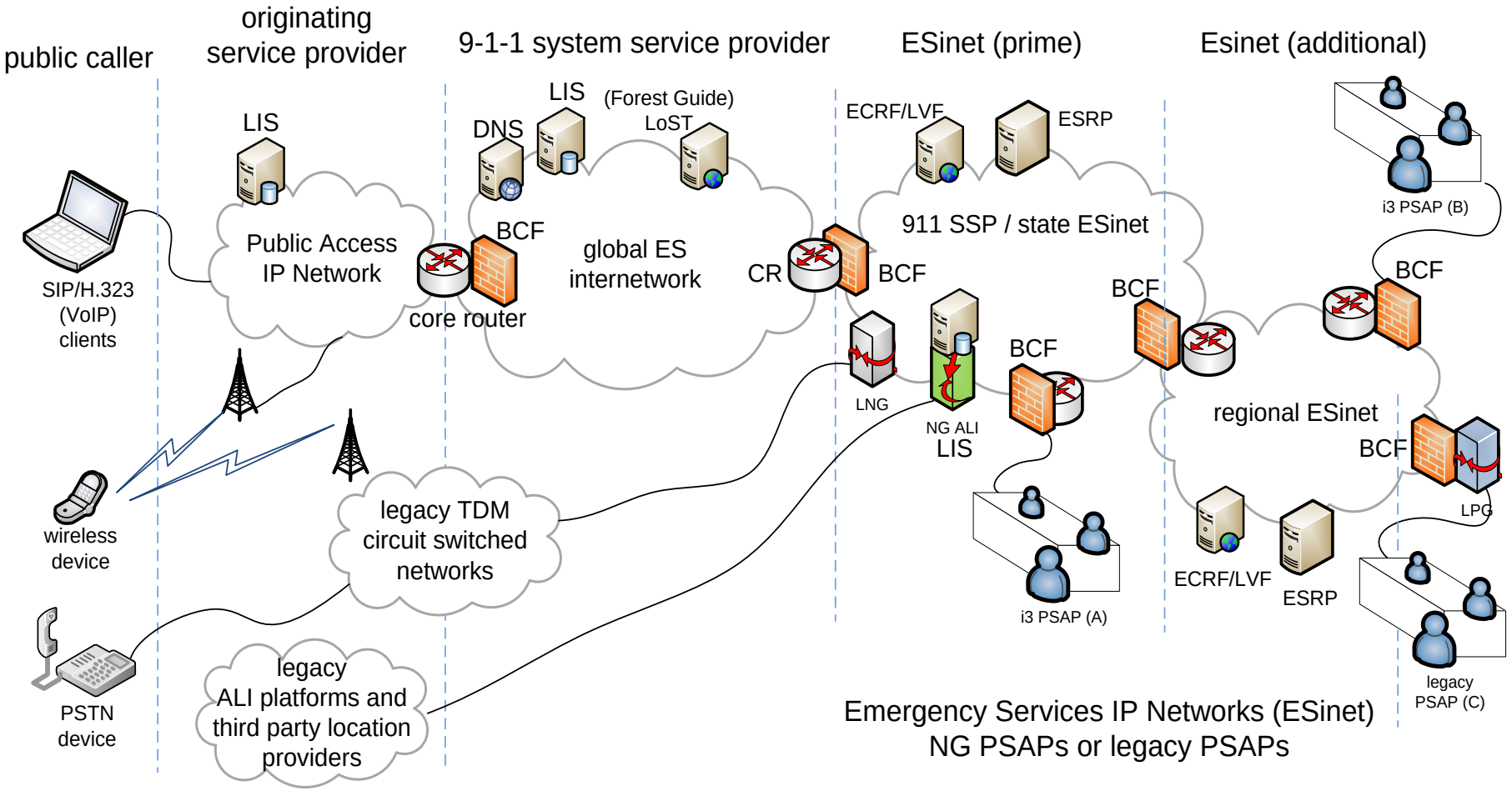
OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

Evolution of 911

	Today's E911	NG911
Networks	Complex Analog Trunking and Data Network	Managed Private Emergency Services IP Network (ESInet)
Routing	Class 5 Switch for Selective Routing	IP Selective Routing function
Accepted Media	Voice Calls Only	Voice, Text, and Video
Integration & Compatibility	Complex Interfaces to Originating Services	Standard IP Interfaces for All Call Types
Bandwidth	20 Character Data Limit	Very large, Broadband Data Bandwidth
Location Services	Routing Based on Translation from Caller Phone Number	Routing Based on Translation from Caller Location

How 911 Will Work Tomorrow – TDM - i3 Diagram



This diagram represents a basic and TDM transitional NG9-1-1 architecture.

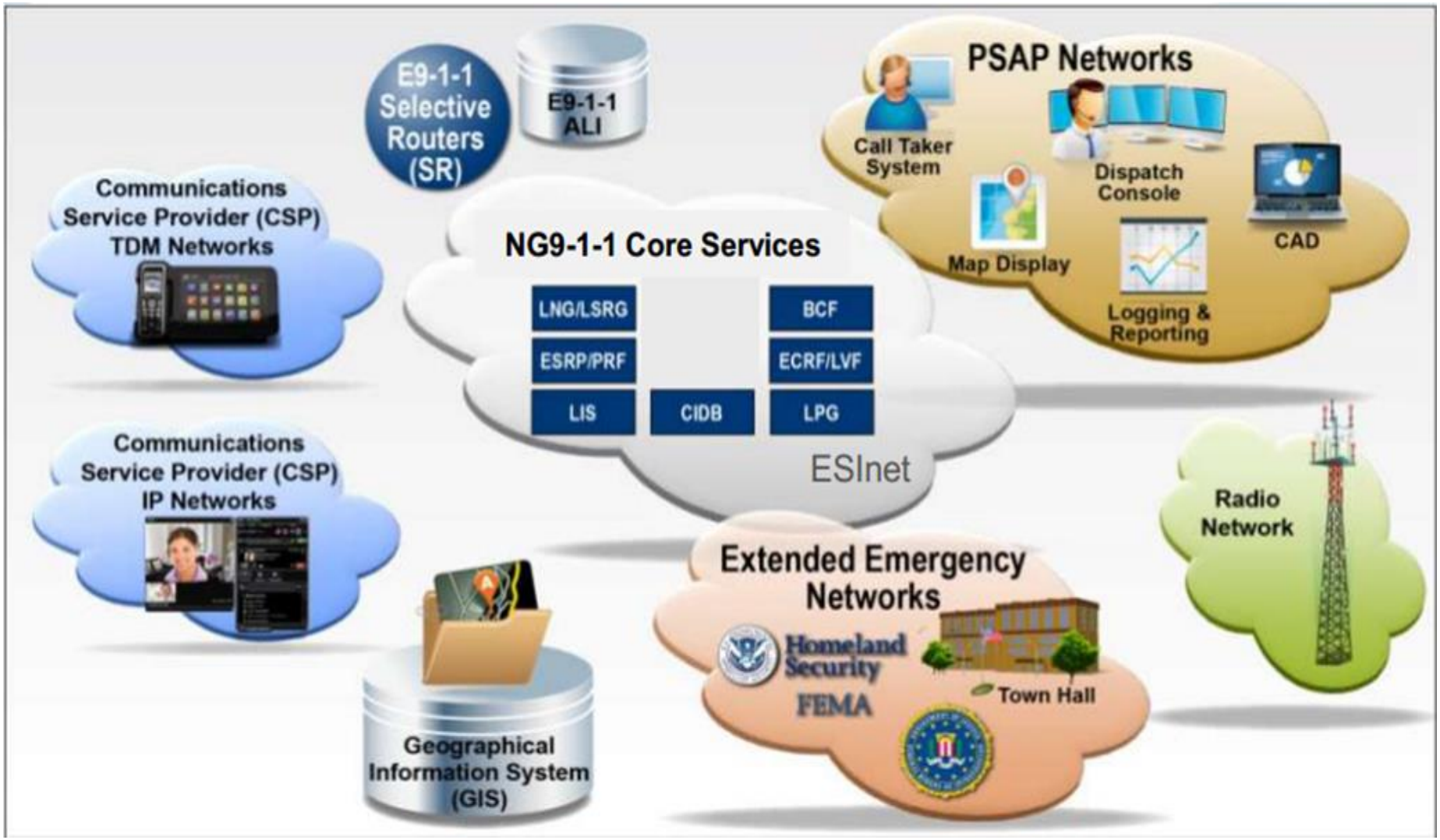
The objective is to demonstrate how a hiearchical distribution of functional elements facilitate a public caller's ability to be routed to the proper PSAP.

Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

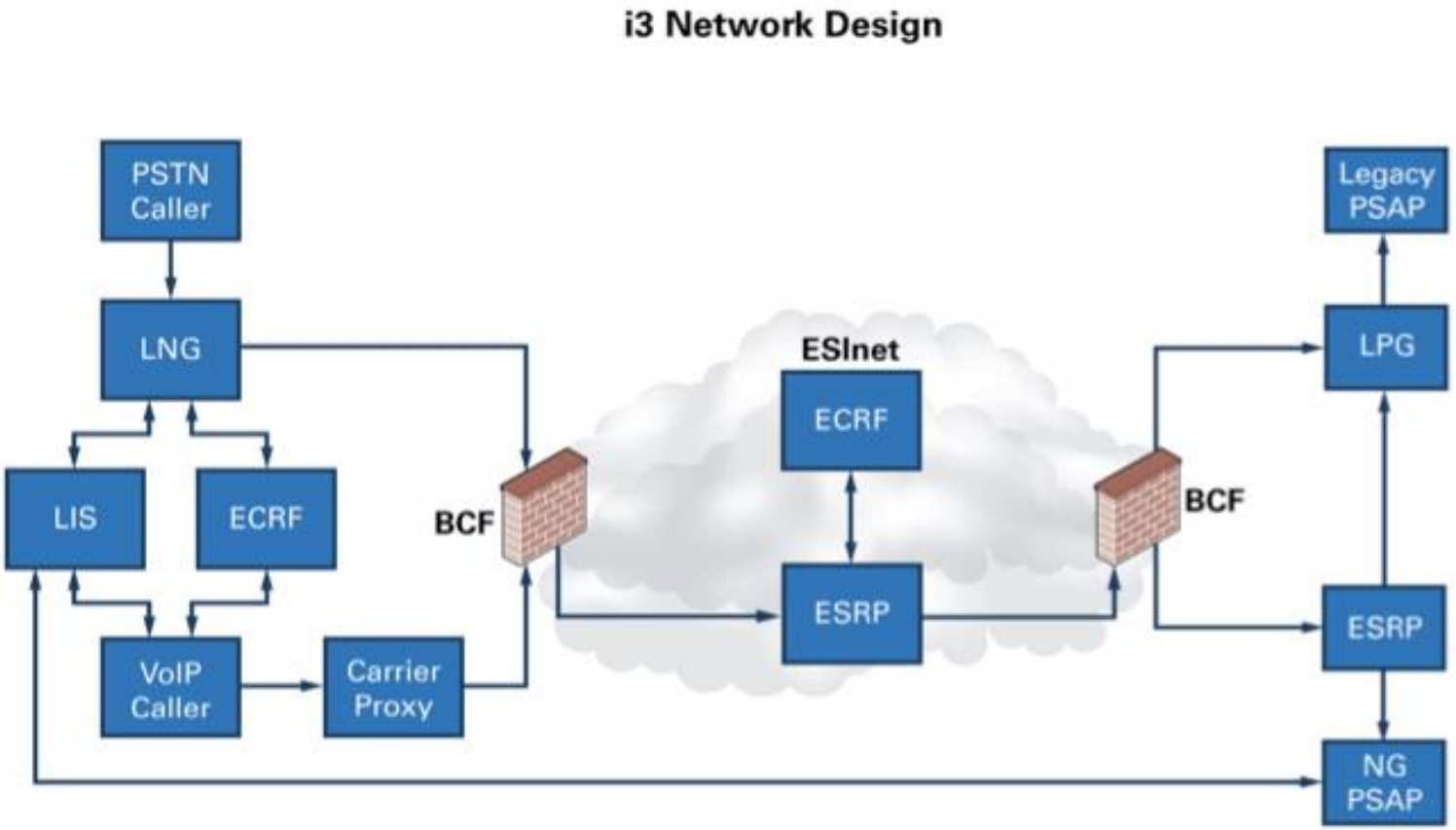
NG911 Ecosystem



ESInet

- An IP-based inter-network (network of networks) shared by all agencies which may be involved in any emergency.
- Entry level foundation for advancement into NG 9-1-1 functions
- Communications components that provide for the transport of traffic across the network
- Normally MPLS but can be a hybrid of technologies based upon the solutions available
- Provides direct connectivity to all PSAP's in the ESInet

Simplified diagram

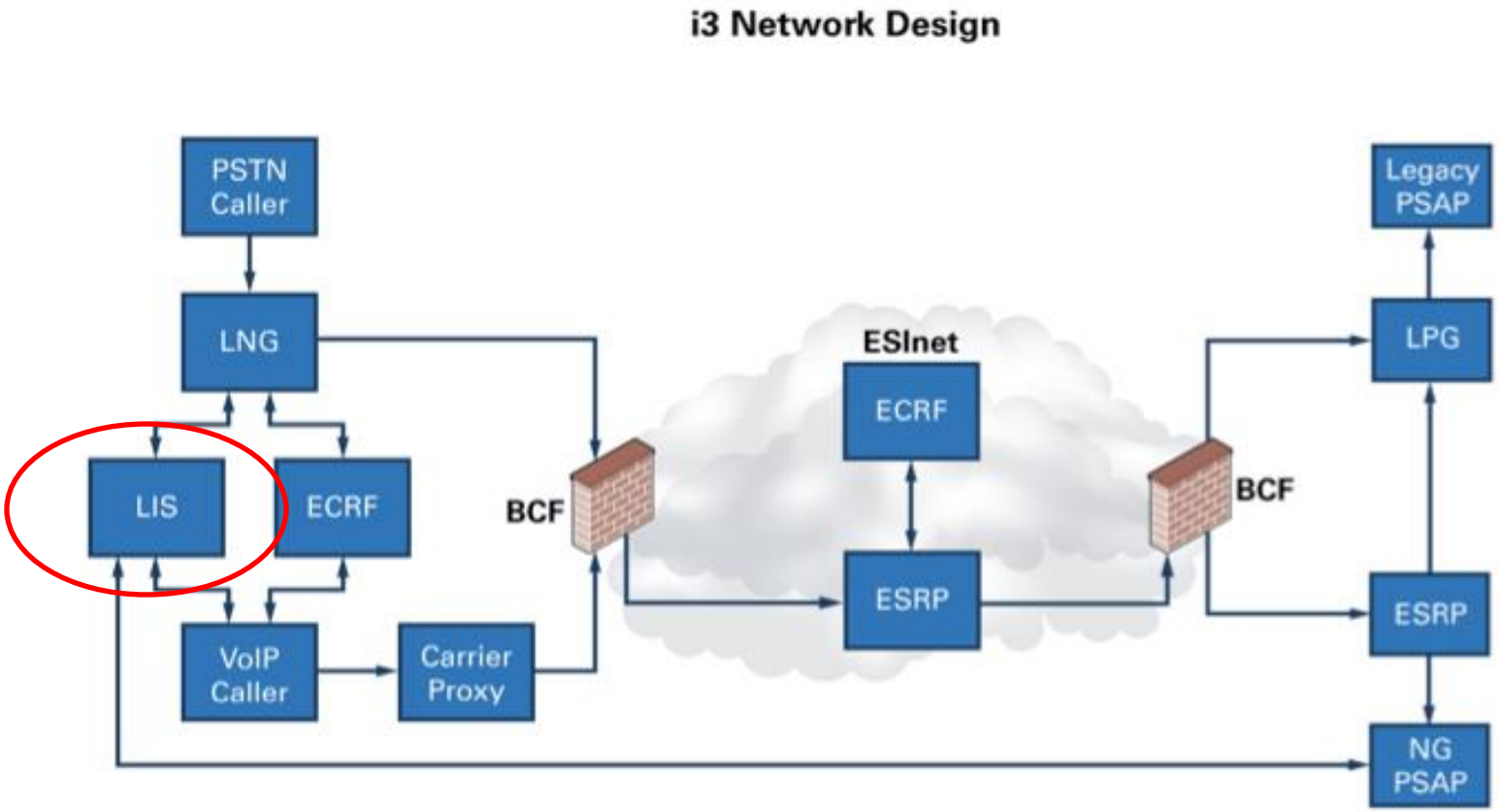


Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

Simplified version of i3



Homeland Security

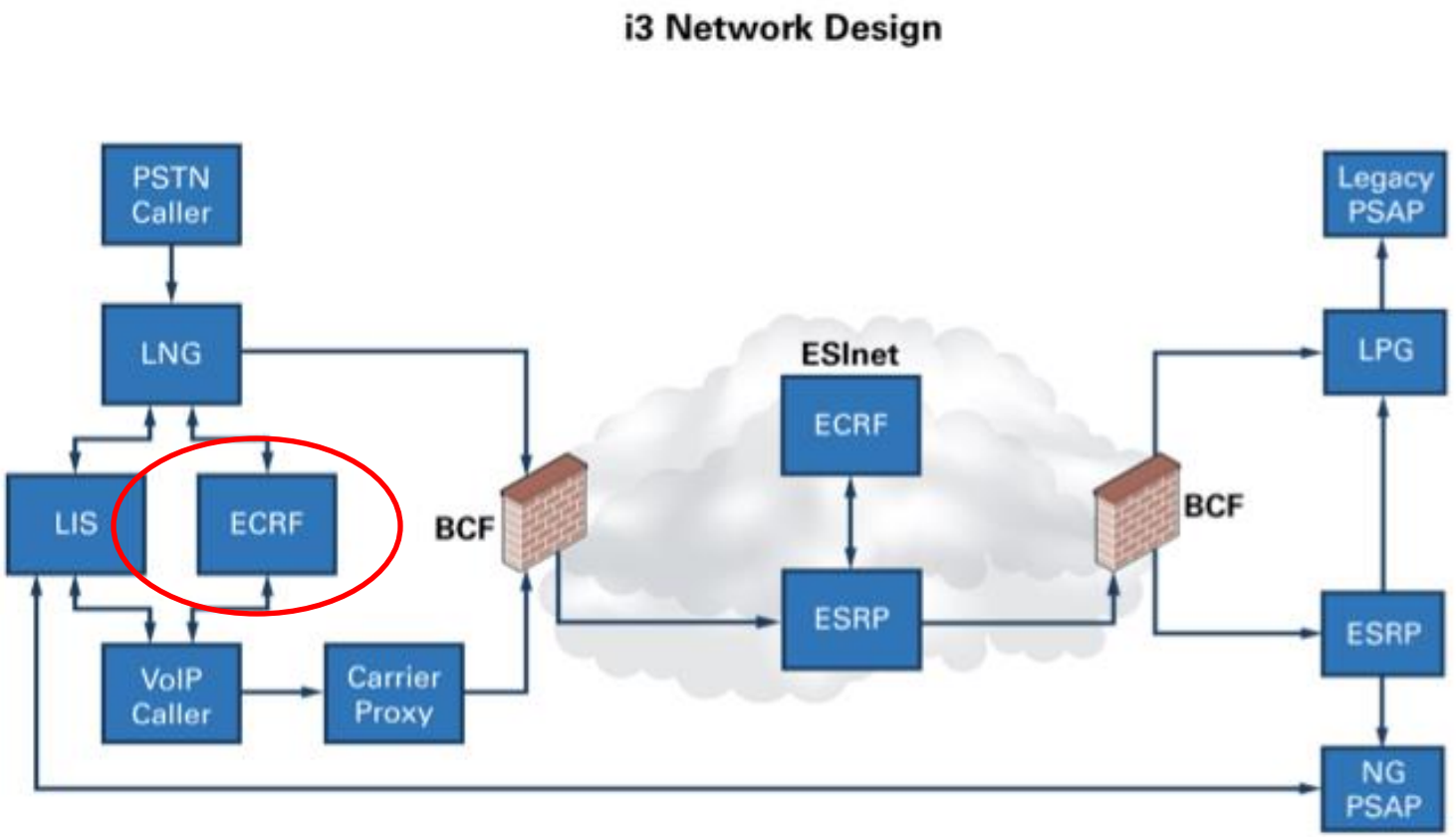
OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

Location Information Server (LIS)

- Each service provider maintains a LIS
- LIS is a server that stores a location based upon a key
- Key can be
  - IP address
  - MAC address
  - Telephone Number (mostly for legacy wireline)
- Each device queries the LIS when it boots, and periodically thereafter (especially when moving) and before a call
- Returns a PIDF, (Presence Information Data Format), the new form of location
  - Civic (street address) or geo (X,Y)
  - Location by value/location-by-reference

Simplified version of i3



Homeland Security

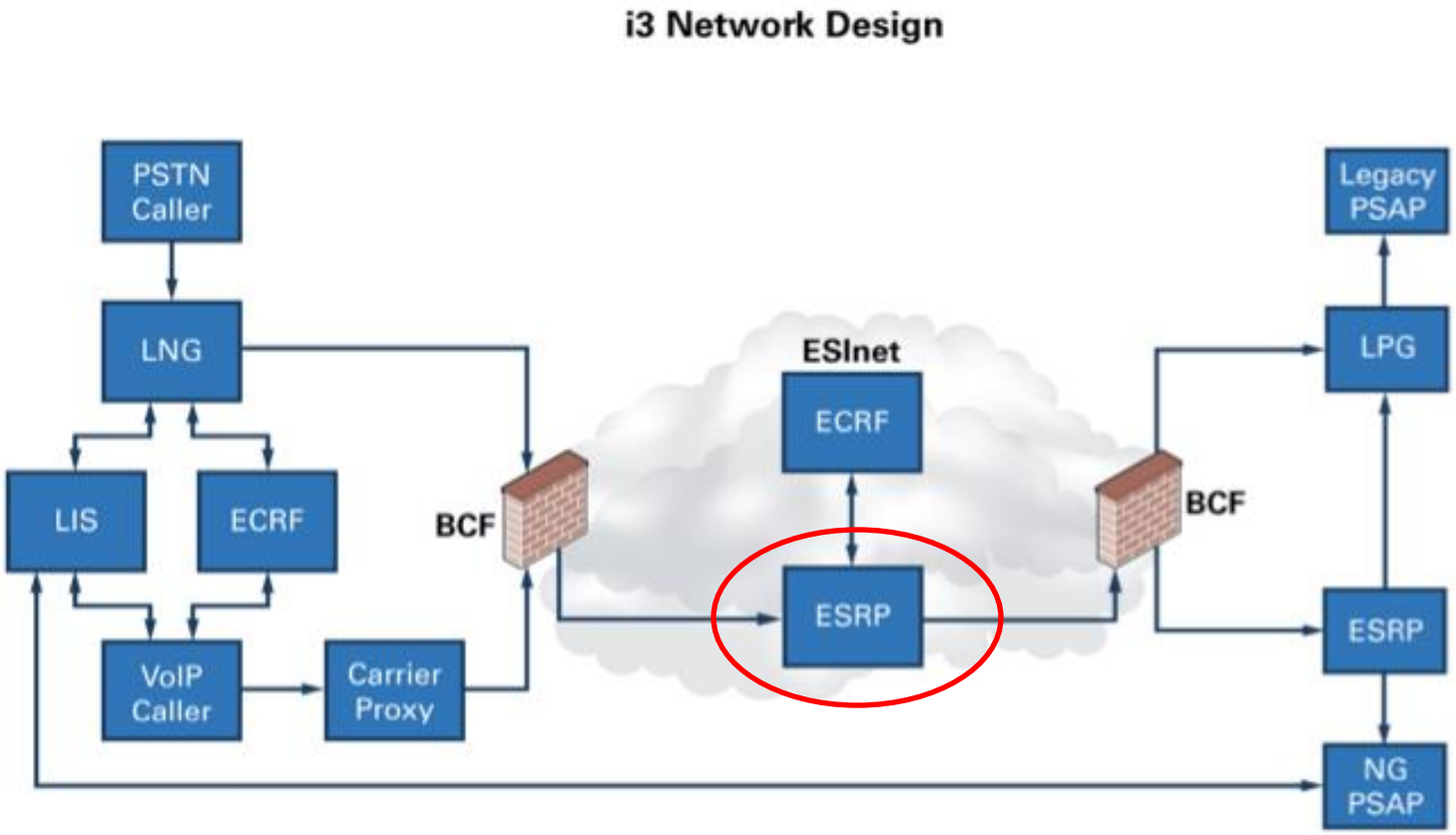
OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

Emergency Call Routing Function (ECRF)

- NG9-1-1's routing database – functions similar to selective routing
  - Uses Location to Service Translation (LoST) protocol to query data
  - Replaces MSAG and ESN codes
- External ECRF routes to correct ESInet (and to the ESRP next slide)
- Internal ECRFs route to correct PSAP
  - ECRF also used to route to correct Police, Fire, EMS, etc
- Provisioned from the 9-1-1 Authority GIS (State, Regional and Local)
  - Polygons define service boundaries
  - On line, real time updates - Useful in disasters
  - GIS gets a "Web Feature Service" interface auto-provisions the ECRF (and LVF)
  - State ECRFs and the National Forest Guide
- Replication across interconnected ESInets

Simplified version of i3



Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

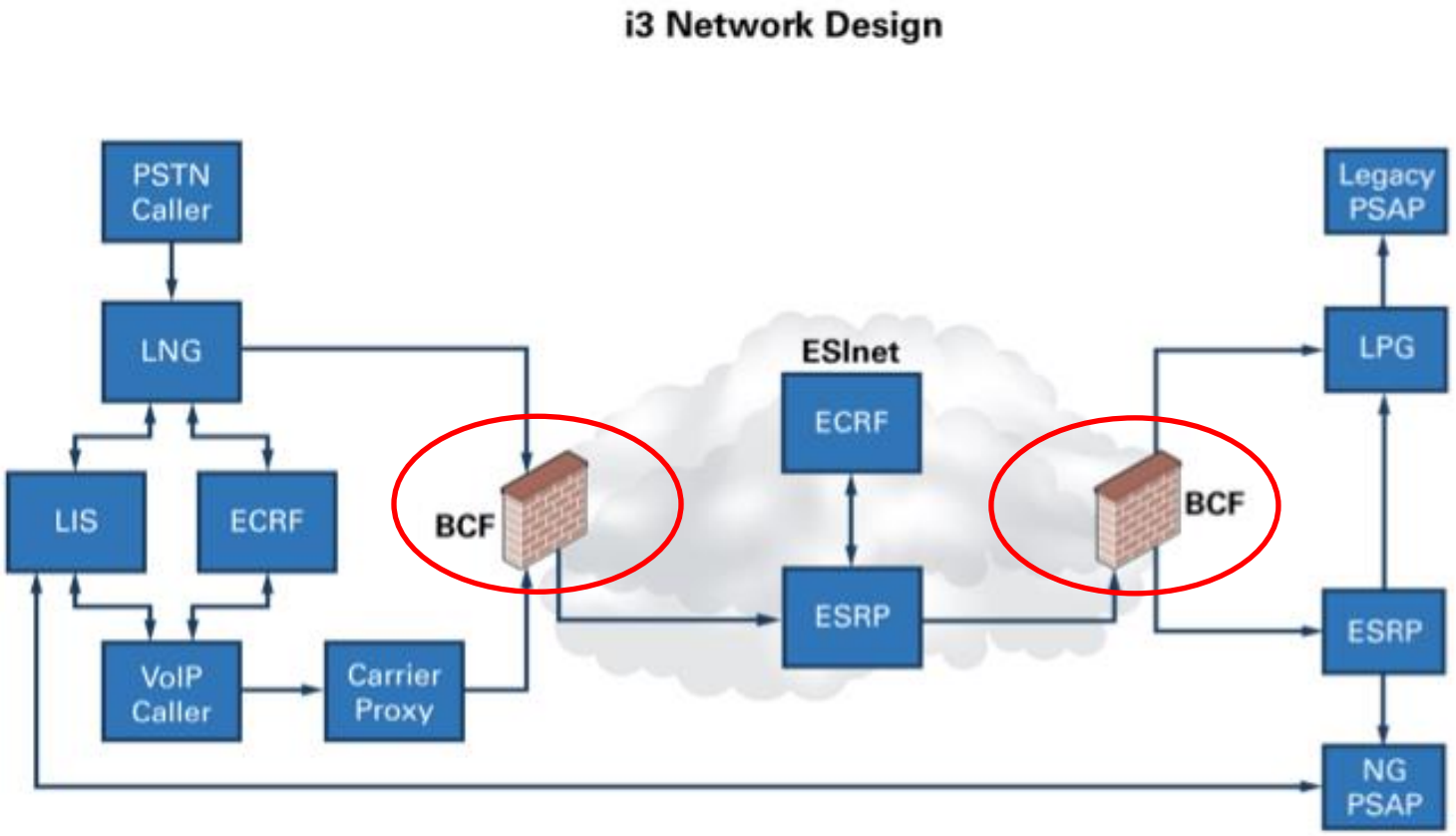
Emergency Services Routing Proxy (ESRP)

- Functions at the Core of the NG9-1-1 network
- In NG9-1-1, the closest thing to the Selective Router
  - Uses the ECRF to choose a nominal next hop
  - Applies the route policy of the nominal next hop to determine actual next hop
- Route policy can be according to account state of PSAPs, congestion, media, source, suspicion level, etc

Policy Routing Function (PRF)

- PSAP controlled rules for how calls are routed in ESRP
  - Inputs are PSAP state, congestion state, security posture, call suspicion, call state (SIP headers and additional data), etc.
  - Output is a routing decision
- ESRP queries ECRF with location for “nominal next hop’. That entity’s policy is fetched from a policy store and interpreted
  - Policy is dynamic = change it at any time, new calls route with new rules
  - Policy rules have a standardized format

Simplified version of i3



Homeland Security

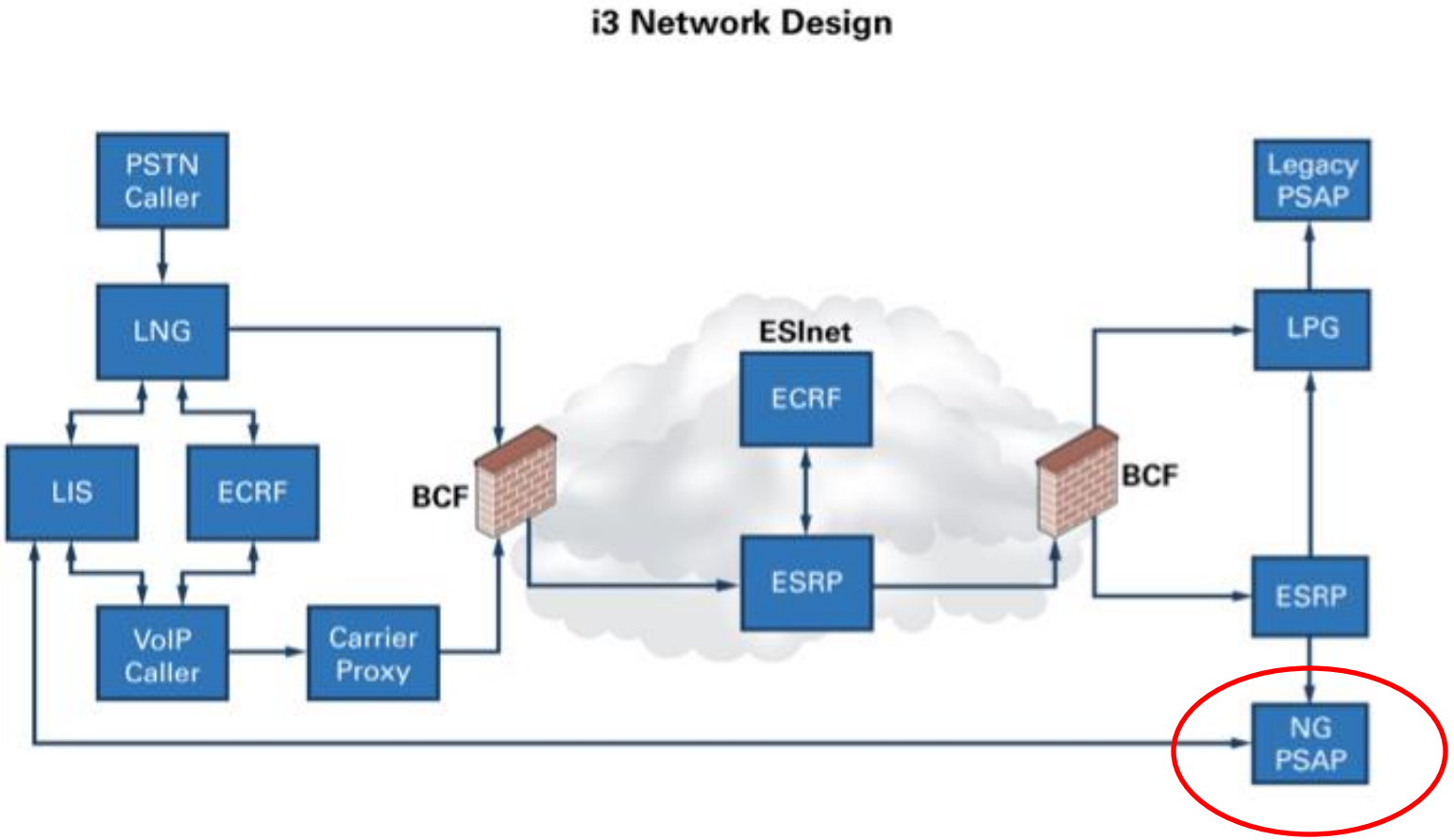
OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

Border Control Function (BCF)

- External security border for ESInet
- Internal isolation border for PSAP
  - Has both firewall and Session Border Controller (SIP specific) parts
- ESInet BCF must withstand largest feasible attack (currently in the range of 10G)

Simplified version of i3



Homeland Security

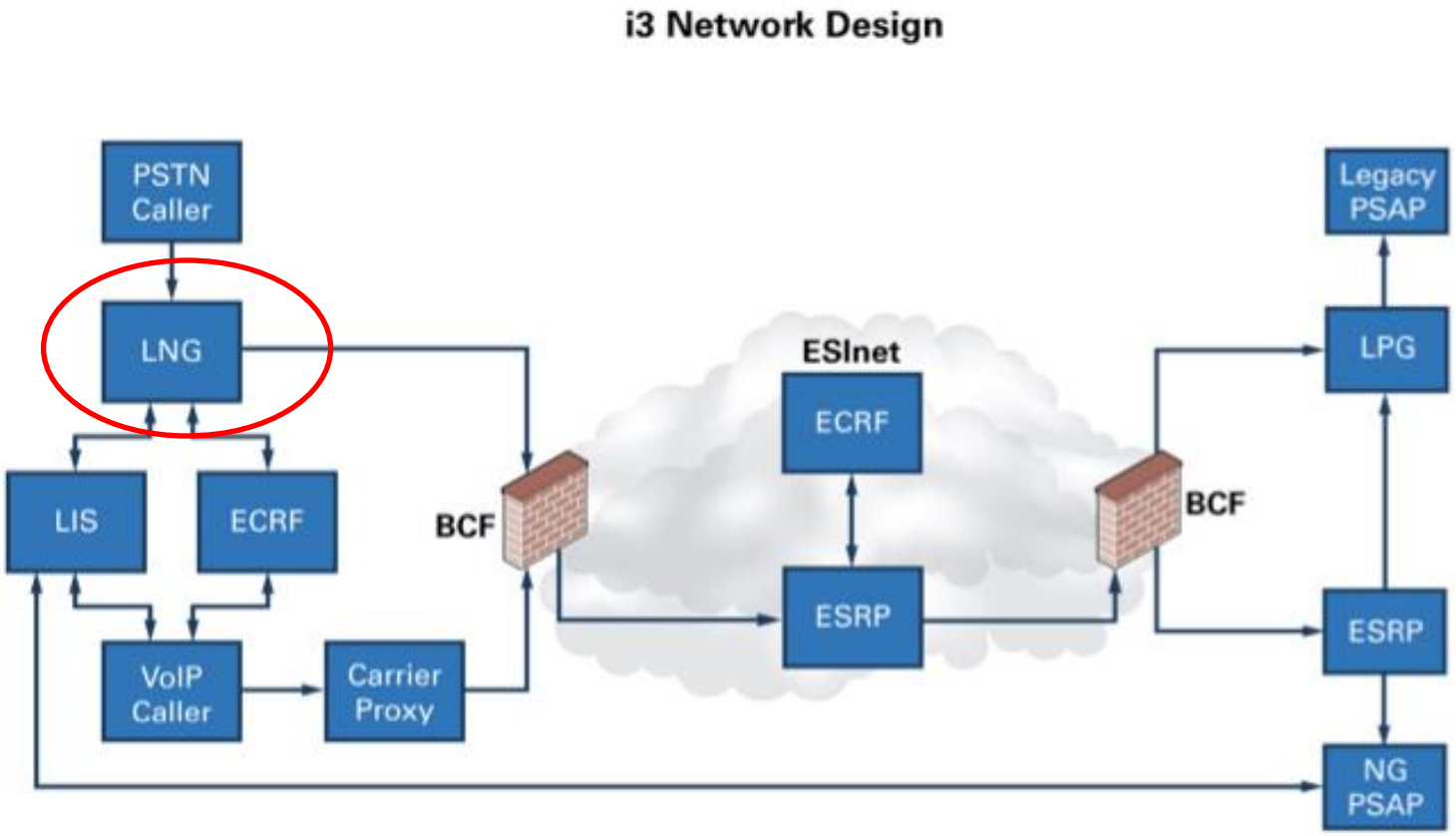
OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

i3/NG PSAP

- Gets all calls from the ESInet
  - SIP
  - With location (does not query ALI database)
  - Routed by ECRFs
- Can use ECRF/ESRP to route to queues of call takers
- All i3 PSAPs are multimedia capable = voice, video, text
  - Virtual PSAPs
- Calls routed to responding agencies with ECRF

Simplified version of i3



Homeland Security

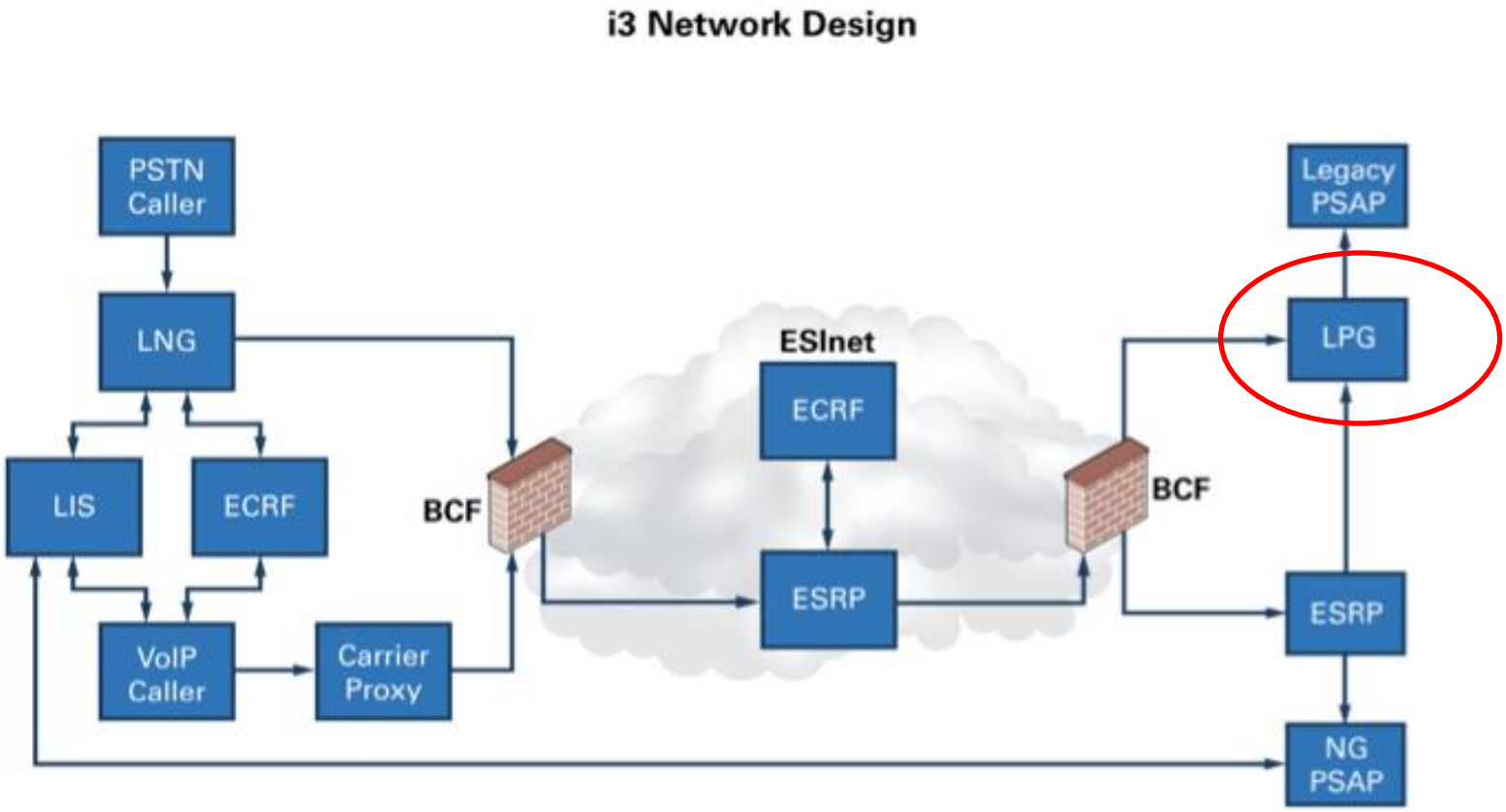
OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

Legacy Network Gateway

- Bridge between existing origination network and ESInet
- SR interface towards the origination network (ISUP or CAMA), SIP interface towards ESInet
  - Outside ESInet, routes via ECRF, always. Comes through the BCF, always. Always uses the ESRP, always
- A permanent part of NG9-1-1, as long as legacy origination networks are deployed

Simplified version of i3



Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

Legacy PSAP Gateway (LPG)

- Allows existing, un-upgraded PSAP to connect to ESInet
- Full NG/SIP interface towards ESInet, SR/ALI interface towards PSAP
- No upgrades needed at PSAP, but needs a GIS compatible with NG functions
- Used as a temporary measure after SR is decommissioned when some PSAPs aren't yet upgraded

Location Validation Function (LVF)

- Used by LIS to validate location before loading it into the LIS
  - Like MSAG validation, but uses the Presence Identification Data Format / Location Object (PIDF-LO) based
  - PIDF-LO is a SIP based location framework
  - Exactly like ECRF, same protocol, same data
- PIDF-LO can validate to street address (not just address range)
- PIDF-LO can validate to building/floor/unit/room

Dispatch

- There are no ESZ/ESNs in NG9-1-1
  - A query of the ECRF with the location of the caller and a “service urn” for the service you want (police, fire, …)
- Not limited to police/fire/ems
- Driven by service area polygons in the GIS
- Adding new services, and adding/modifying polygons is relatively easy
- NG9-1-1 is still processing, handling and delivering *9-1-1 calls/requests*

CAD

- New, expanded interfaces to CAD
- Allows Call taker to CAD; and CAD to CAD data interchange
- Standardized interfaces
  - Mutual aid doesn't require common vendors to request dispatch
- Any call can be answered by any PSAP and all data needed to handle the call, and supply data to responders is included

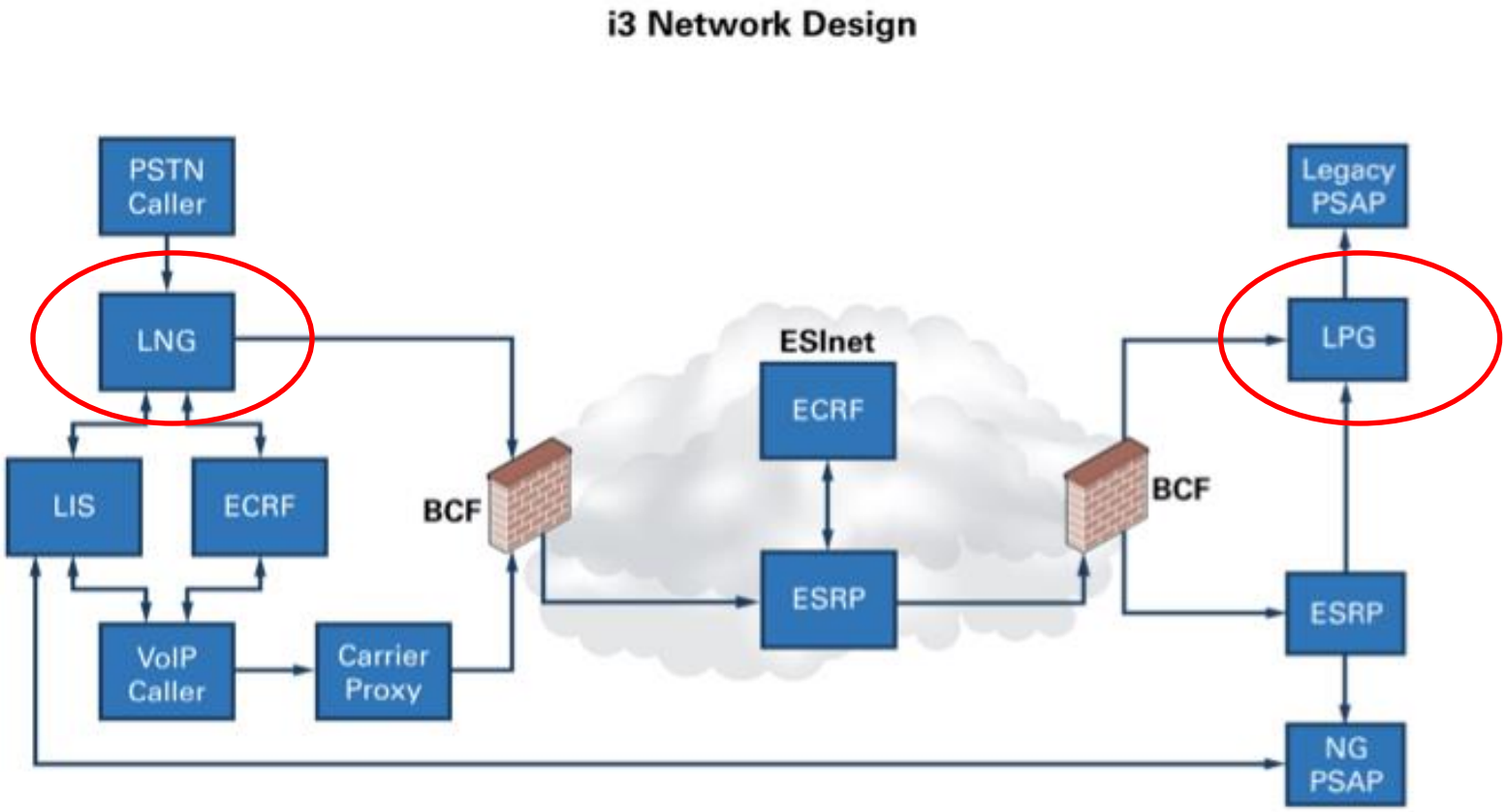
Security

- Security is extremely important in NG9-1-1
- The ESInet may be connected to unsecure external networks
- ALL protocol interactions must be encrypted and authenticated
  - Single Sign-on
  - Policy driven Data Rights Management
- Credentials matter
  - Everyone gets his own

The Technology Transition

- There is no fork lift upgrade nationwide to NG9-1-1
- PSAPs and carriers will migrate over some period of time
- NENA has identified two paths to migration
  - Legacy Selective Router Gateway
  - IP Selective Router

Simplified version of i3



Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

Legacy Selective Router Gateway

- Tandem to Tandem transfer between SR and ESInet
  - Calls originated on a carrier connected to SR can terminate on an i3 PSAP
  - Calls originated on a carrier transitioned to i3 can terminate on a legacy PSAP connected to the SR
  - Calls can be transferred among i3 and legacy PSAPs
- Allows carriers and PSAPs to transition, in any order
- When the last carrier and PSAP transition, the SR is decommissioned
- Allows location queries across the ALI/LIS boundary

IP Selective Router

- Replace existing SR with a new SR that has new capabilities
- Gradually evolve PSAPs and carriers to i3 interfaces
- One fork lift upgrade in an area + some number of incremental upgrades
  - Not standardized – vendor free for all
- Beginning and end state are defined, but not how you get there
- Could have multiple upgrade steps for each party

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
  - Creates individual sessions across the network to facilitate the delivery of voice, text, data and video
  - Chosen as the call delivery method for Voice over IP
  - Selected as the building block for NG 9-1-1
  - Generally can be used to build NG 9-1-1 as an application that uses the ESInet for connectivity
- SIP sets up the path for a call – collects all of the data about the call – then carries the call through the network to the destination – and delivers all the information about the call

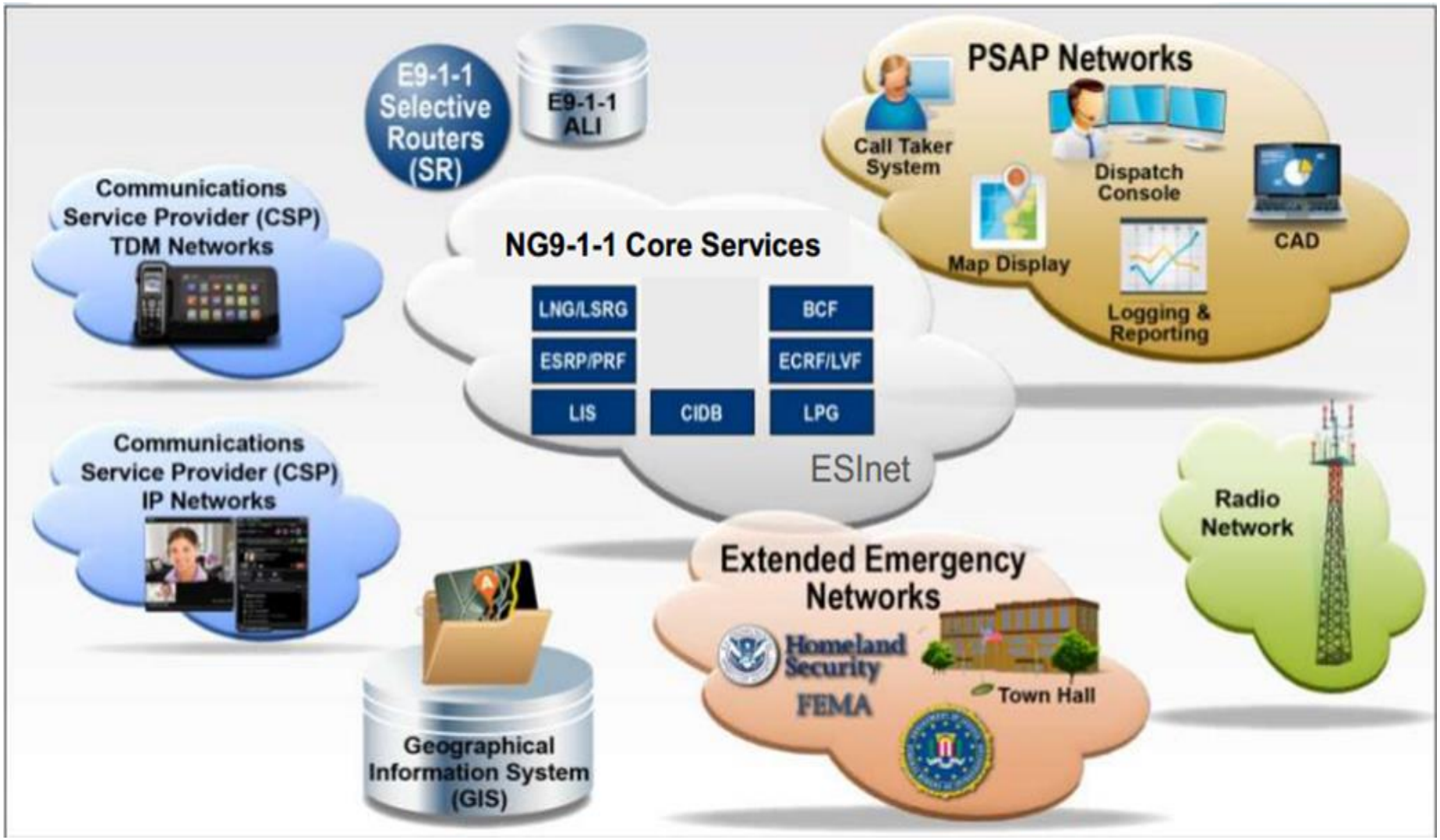
Operational Impacts of NG911

Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

NG911 Ecosystem



Example NG911 Stakeholders

- Citizens
  - Access 911 from any device
  - Additional and better information related to incident
  - Direct notification and better situational awareness
- Federal, State and Local Government
  - Public Safety
    - Quicker and more precise response
    - Integrated Command and Control
    - New applications and tools
    - Access to additional media and data
  - Regulatory
  - Policy
  - Elected Officials
- Standards Bodies
- Non-Profit Organizations
  - American Heart Association
  - American Red Cross
  - National Center for Missing and Exploited Children
- Educational Institutions
- Regulated Telecommunications Providers
  - Wireline
  - Wireless
  - VoIP
- 911 Service Providers
  - Network
  - CPE
  - Applications

Community Expectations

- Same 911 access & service regardless of location, device
- High standards and requirements
- Reliable equipment & processes, esp. in disasters
- Warning notifications on social media, multimedia devices
- Equal access for special needs community

NG911 Myths and Truths

- There are several myths and misconceptions encountered when discussing NG911—
  - The PSAP working environment will change radically overnight
  - Accurate location data is guaranteed
  - NG911 will immediately begin to save money
  - Harassing or malicious 911 calls will be eliminated

- Instead, NG911 is—
  - Migrating 911 from Legacy Circuit-Switched Technology to IP solutions
  - Establishing interconnected broadband networks for the processing and routing of calls for service and information exchange between agencies
  - Embedding location data in each call for service (No need to query databases)
  - Implementing dynamic management of call routing policy (operator loading, time-of-day, malfunctions, etc.)
  - Modernizing PSAP CPE (as needed)

NG911 Improvements and Capabilities

Expand PSAPs and E911 Center capabilities

- Transfer voice and data between all NG911 PSAPs nationwide
- Directly activate alternate routing to control call volume
- Access a wide range of databases to expand data sharing and facilitate emergency response and comprehensive incident management

Enhance capability of current and new originating devices

- Non-voice messaging of various types
- Text-to-911
- Devices, such as sensors, generating data-only messages
- Photo and video transmission
- Telematics

Fully integrate and interoperate with other emergency systems and entities

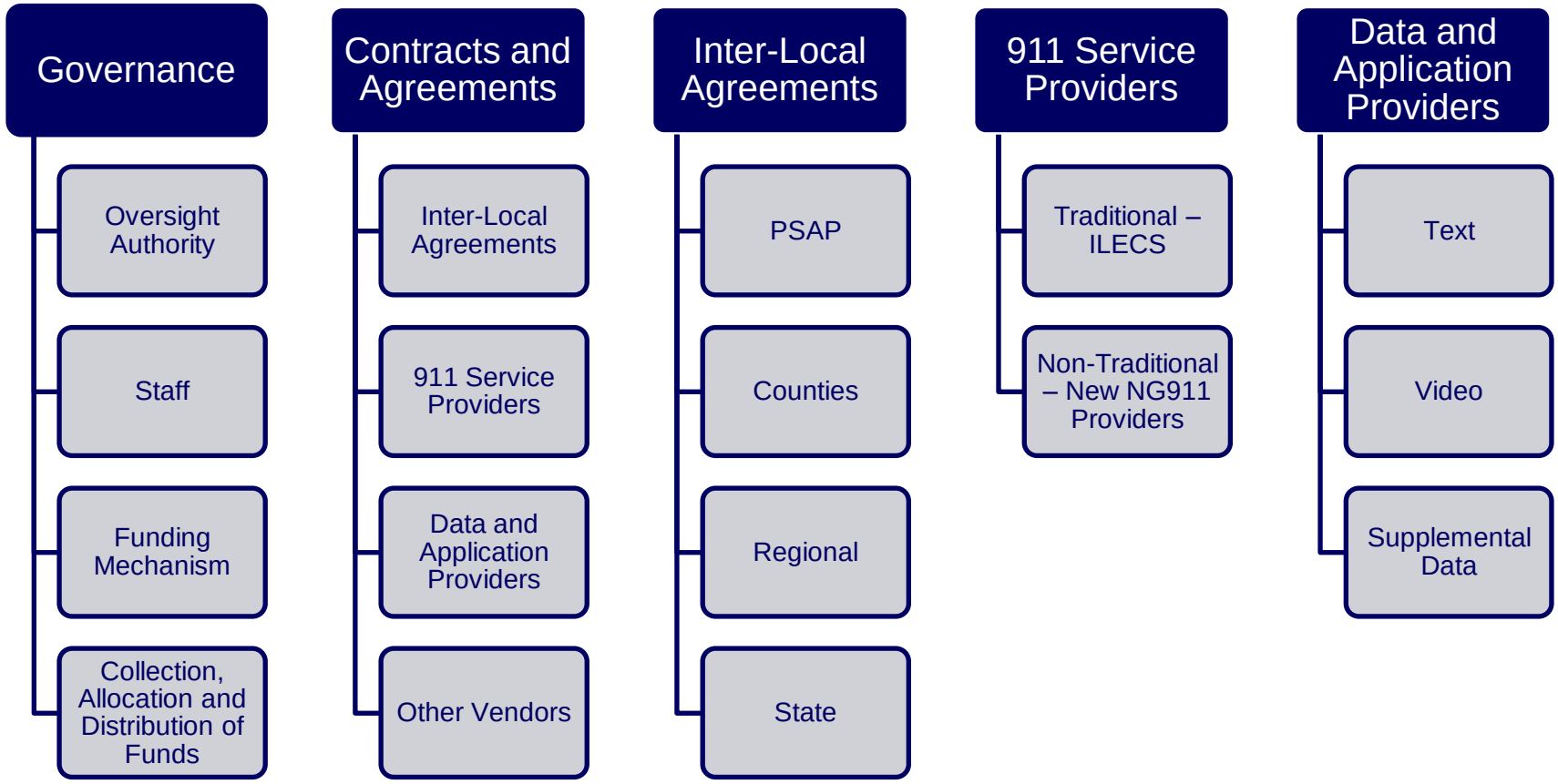
- Other PSAPs
- Emergency Operations Centers
- DHS and other emergency management entities

Homeland Security

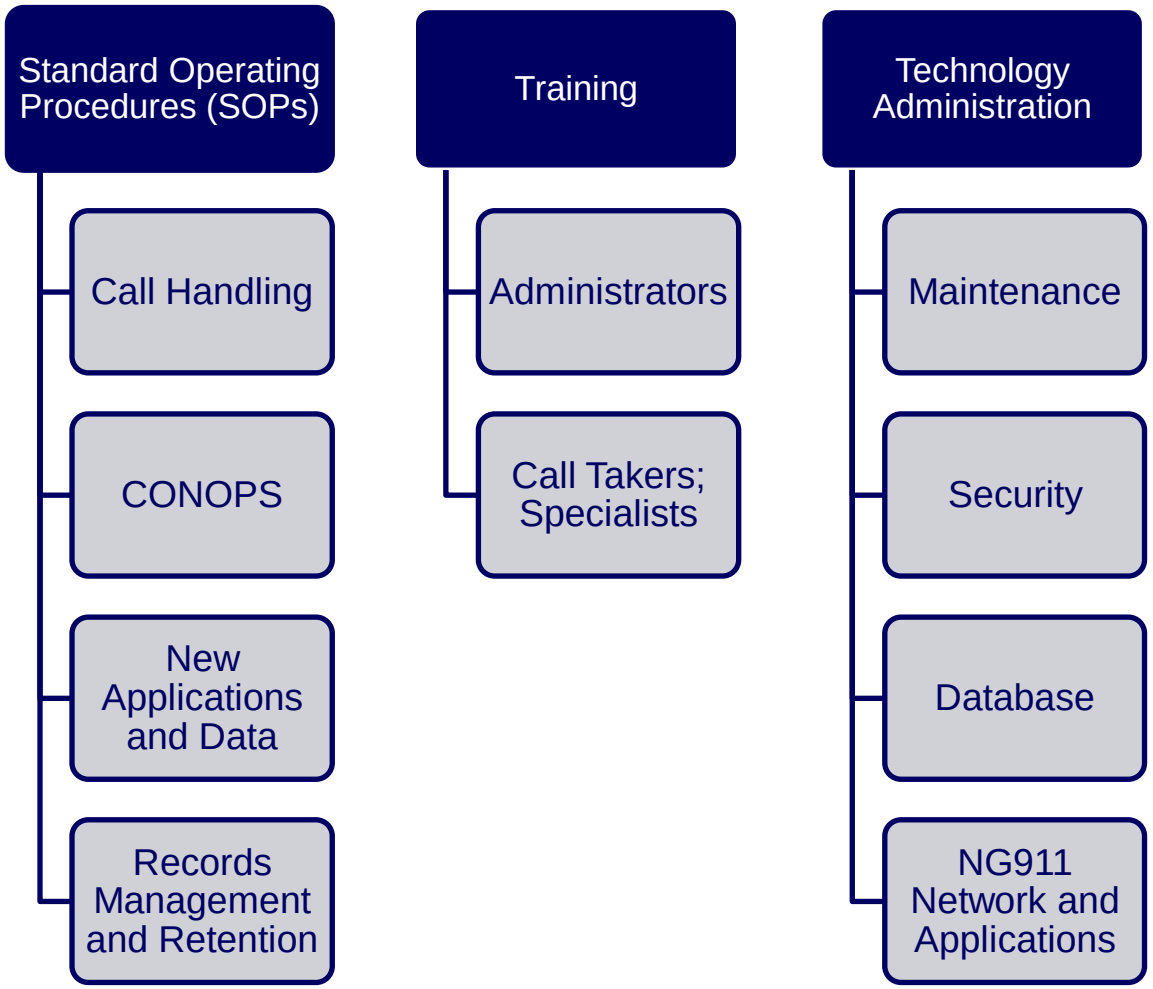
OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

Governance and Operational Impact



Governance and Operational Impact



Dealing with other systems

- Can’t realistically upgrade every system in the PSAP at the same time
  - Some legacy systems have to live in an i3 world
  - Implies MSAG style addresses are still needed
  - MSAG Conversion Service converts PIDF to MSAG and vice versa
- Extra attributes in the GIS system
  - Additional layers to help response and protection efforts
  - Ability to visually see the correlations impacting public safety

NG9-1-1 Landscape
Text-to-911

FCC Interim (Pre-NG911) Text-to-911 Rulemaking

- In December 2012, AT&T, Verizon, Sprint and T-Mobile agreed on a joint commitment to provide national text-to-911 capabilities to PSAPs by 2014
  - Under the agreement, text-to-911 services will be made available for the public and for Public Safety Answering Points (PSAPs) no later than May 15, 2014; however, the service will not be available to subscribers roaming outside of their home wireless network
  - In addition, carriers were required to implement bounce-back messages by June 30, 2013 in areas where text-to-911 service is not available to consumers
  - The joint agreement also outlined commitments by the carriers to work with APCO, NENA and the FCC in providing education regarding availability and limitations of text-to-911 services to the public, as well as text-to-911 training for PSAPs
- Under the agreement, carriers are obligated to submit quarterly text-to-911 progress reports outlining deployment status and milestones
  - The quarterly status reports can be found at the FCC web site

Short Message Service (SMS)

- Carrier native SMS is the most commonly available texting technology today.
- Can be supplied by carrier
  - Does not require a third party texting or messaging application.
- Wireless customers can send and receive text messages using the single code “911”.
- Provide text capability to PSAPs without additional software or hardware costs.

SMS Limitations

- Does not support photos, videos, or multiple recipients for text messaging.

- Interim SMS Text-to-911 will not be supported when a subscriber is roaming.*

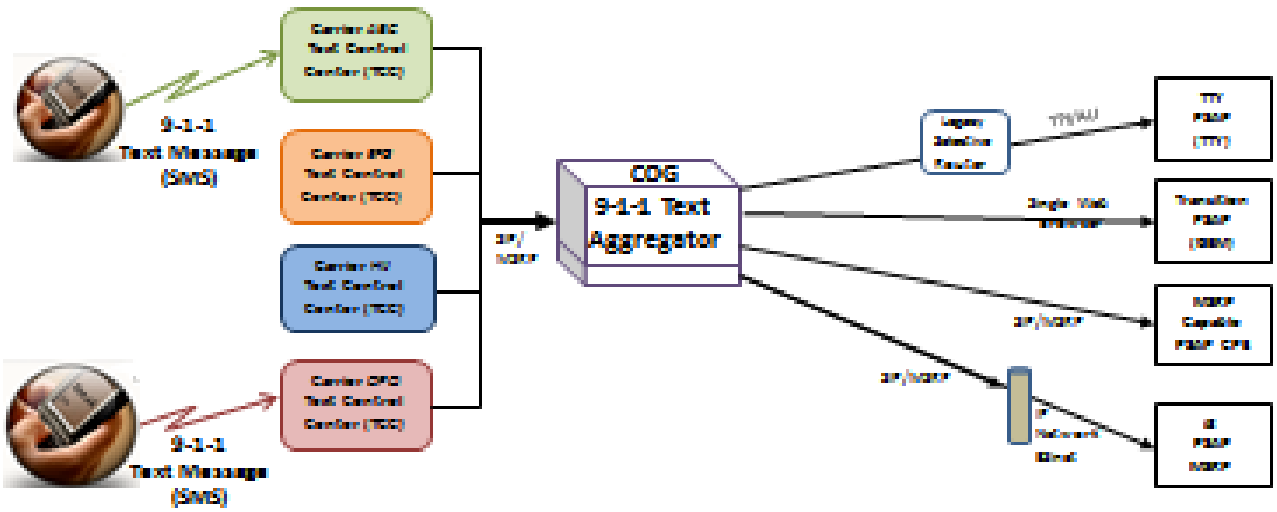
***Roaming** means the subscriber is receiving wireless service from any carrier other than his/her home carrier, regardless of the subscriber's current location.*

Text-to-911 Location Accuracy

- The wireless carrier and their Text Control Center provider route text messages to the appropriate PSAP over the selected interface based on the cell sector, and they provide the PSAP with a latitude/longitude location of the calculated centroid for the center of the cell sector RF coverage (e.g. coarse location) using commercial location positioning service.
- More precise Texter location may be available, but is carrier-/vendor-implementation specific.

One Approach to Text-to-911

Metropolitan Washington Council Of Governments (COG)
9-1-1 Director's Strategy for Implementing Text to 9-1-1



Strategy:

- Efficient. Aggregates all Text-to-9-1-1 traffic from multiple wireless carriers and TCC vendors, allowing COG PSAPs to interact with a single servicing provider for Text-to-9-1-1.
- Flexible. Supports transfer of text sessions between different text handling protocols.
- Trainable. PSAPs can use a single user interface for Text-to-9-1-1 (TTY, Web or text-enabled CPE) and transition to a new CPE interface without changing the aggregator.
- Industry standard interface. Alliance for Telecommunications Industry Solutions (ATIS) compliant - ATIS/ISTD-110 standard.
- NG9-1-1 compliant. (National Emergency Number Association (NENA) i3 standard).

Exhibit A

Text Control Center (TCC)

Nationally, the wireless carriers and their vendors are deploying Text Control Center (TCC) functions to interface between a carrier-originated wireless 9-1-1 text user and the PSAP environment. The TCC uses some of the functions of core NG9-1-1 system design, with additional specialized functionality to meet the needs of SMS Text-to-911.

When TCCs from different vendors are able to interoperate with each other, PSAPs can connect to multiple carriers through a single TCC.

There are 2 TCCs: TCS and Intrado.

Text-to-911

9-1-1 Vendor Interim Solutions			
WEB-BASED SOLUTIONS	Advantages	Limitations	Deployments
Stand-alone application that runs on parallel network not connected to 9-1-1. Text message sent to carrier server and relayed to PSAP via internet access.	• **No modifications to E9-1-1 system required** • **No dedicated PSAP IP trunking required**	• **Requires public internet access at PSAP** • **Not incorporated into 9-1-1 system**	• **Multiple deployments nationwide**
Text to Voice Gateway	Advantages	Limitations	Deployments
Smart phone app sends text to Call Relay Center. Operator locates caller, calls appropriate PSAP on admin line and relays text message verbally to PSAP via PSAP admin line. Intrado App announced but not yet available for subscription.	• **No modifications to E9-1-1 system required** • **No dedicated PSAP IP trunking required**	• **Requires available admin line at PSAP** • **Requires additional manual process between texting citizen and call taker** • **Requires user to register with smart phone application**	• **None documented at this time**

Text-to-911

9-1-1 Vendor Interim Solutions			
SMS over direct IP to non-IP PSAP	Advantages	Limitations	Deployments
Text message sent from carrier server over dedicated IP trunks to PSAP. Network equipment at PSAP delivers text to telephone system (CPE).	• **Integrated into 9-1-1 telephone system** • **Logging and recording through telephone system**	• **Requires dedicated IP trunk to PSAP** • **Requires additional back-room PSAP equipment** • **Requires text-capable telephone system (CPE)**	• **i-Wireless in Black Hawk County, Iowa currently live**
SMS to TTY	Advantages	Limitations	Deployments
Text sent to carrier server in standard SMS text format. Carrier translates to TTY and delivers to PSAP on 9-1-1 trunk	• **All PSAPs already TTY enabled** • **Native E9-1-1 routing** • **Call logging and recording part of 9-1-1 telephone system**	• **Simultaneous voice and text not available** • **Text may not be available while roaming – bounce back recommended** • **Some TTY setting changes required to prevent garbled transmissions**	• **Verizon state-wide deployment in Maine currently live** • **Sprint trial in 2013 successful in Maine – no longer in place**

Text-to-911

9-1-1 Vendor Interim Solutions			
Native NG9-1-1 Solution/MSRP	Advantages	Limitations	Deployments
	• **Integrated into 9-1-1 telephone system** • **Logging and recording through telephone system**	• **Requires fully-functional IP-based NG9-1-1 PSAP deployment**	• **Verizon in State of Vermont currently operational** • **Deployments in Indiana**

Planning a Transition to NG911

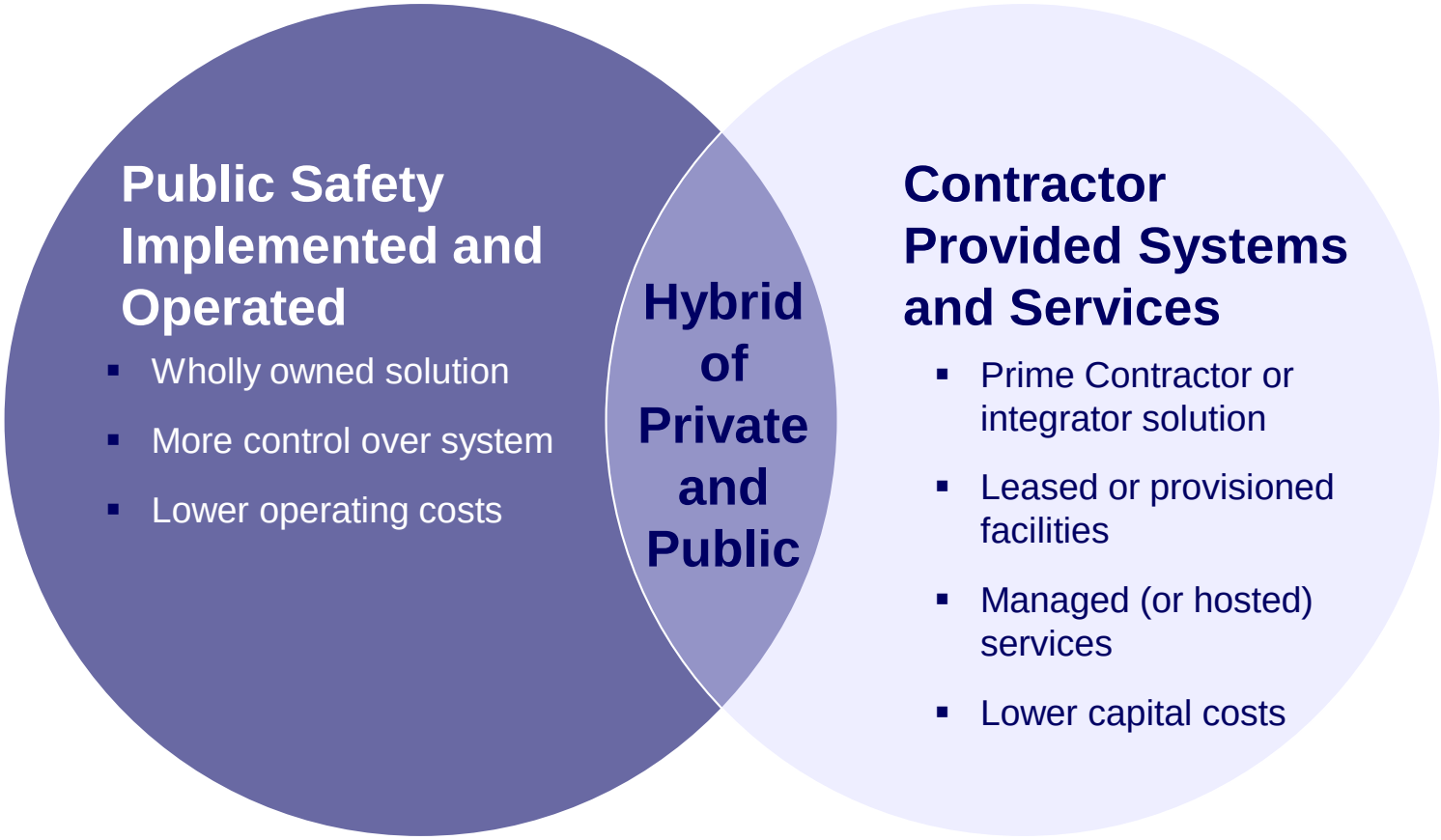
NG911 Realities

- There are many alternative paths for the migration from legacy to NG911
- Coordination among participating entities during transition may be complex and challenging
- Operating costs will be higher during transition because of the need to maintain legacy systems during NG911 deployment
- Education and training of operators and maintainers is essential for success and acceptance
- NG911 standards are evolving as technologies and society evolves
- Interim SMS Text-to-911 solutions are being deployed and the service is becoming wide spread

In preparing for NG911, detailed planning is critical

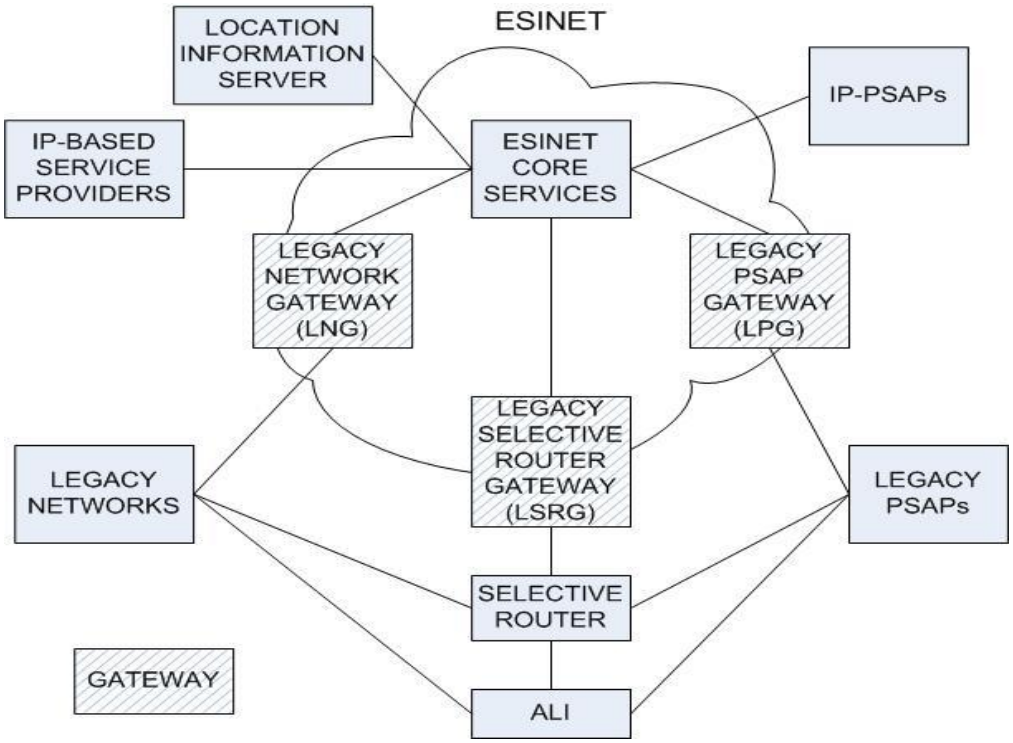
Transition Planning

Business Model Considerations



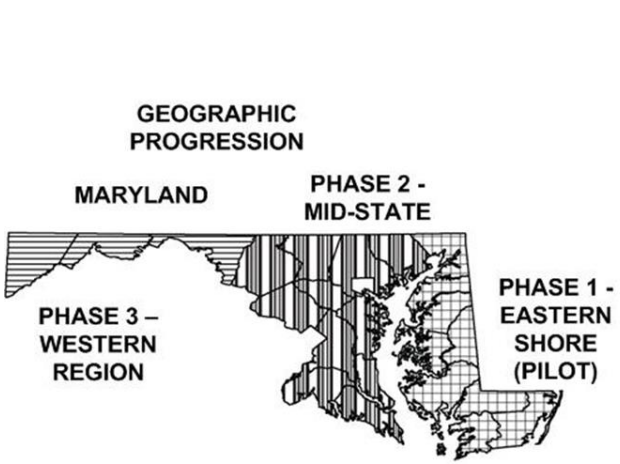
Transition Considerations

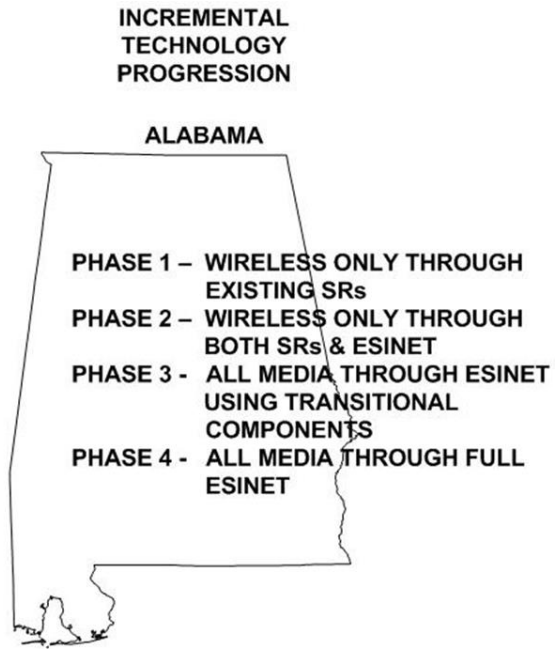
- The objective is a non-disruptive step-wise migration
- Close coordination among all parties is essential
  - OSPs, SSP, PSAPs, and the NG911 administrator
- There will be alternative paths and the most appropriate can be determined through the process leading to a detailed transition plan
  - Development of a detailed transition plan is critical
- During the transition, the legacy databases must be maintained until the migration is complete



NG911 Transition Alternatives

- Two major alternatives for a phased rollout
  - **Geographic Progression –** Each successive phase corresponds to the transition of a geographic area of the state to NG911 implementation
  - **Incremental Technology Progression –** Successive phases correspond to incremental advances in technology leading to full NG911 realization in the final phase
- Each alternative has its advantages
  - In the geographic approach, the first phase can be a pilot for proof of concept
  - In the incremental technology advance, all of the PSAPs are provided with the same level of service simultaneously





NG9-1-1 Landscape Cybersecurity

Targeting of PSAPs

PSAP systems, like NG 911, may be likely targets for cyber-attacks because of their critical missions and access to non-public and personal information

The emergency communications system can be assumed to be a high-value target for hackers, criminals and others seeking to wreak havoc upon the U.S. infrastructure. The good news is that thousands of businesses and public agencies are already using secure IP networks, including healthcare providers and financial institutions that must meet stringent information security compliance requirements.

~ Verizon/Intrado, Emergency Services White Paper

NG 911's Need for Cybersecurity

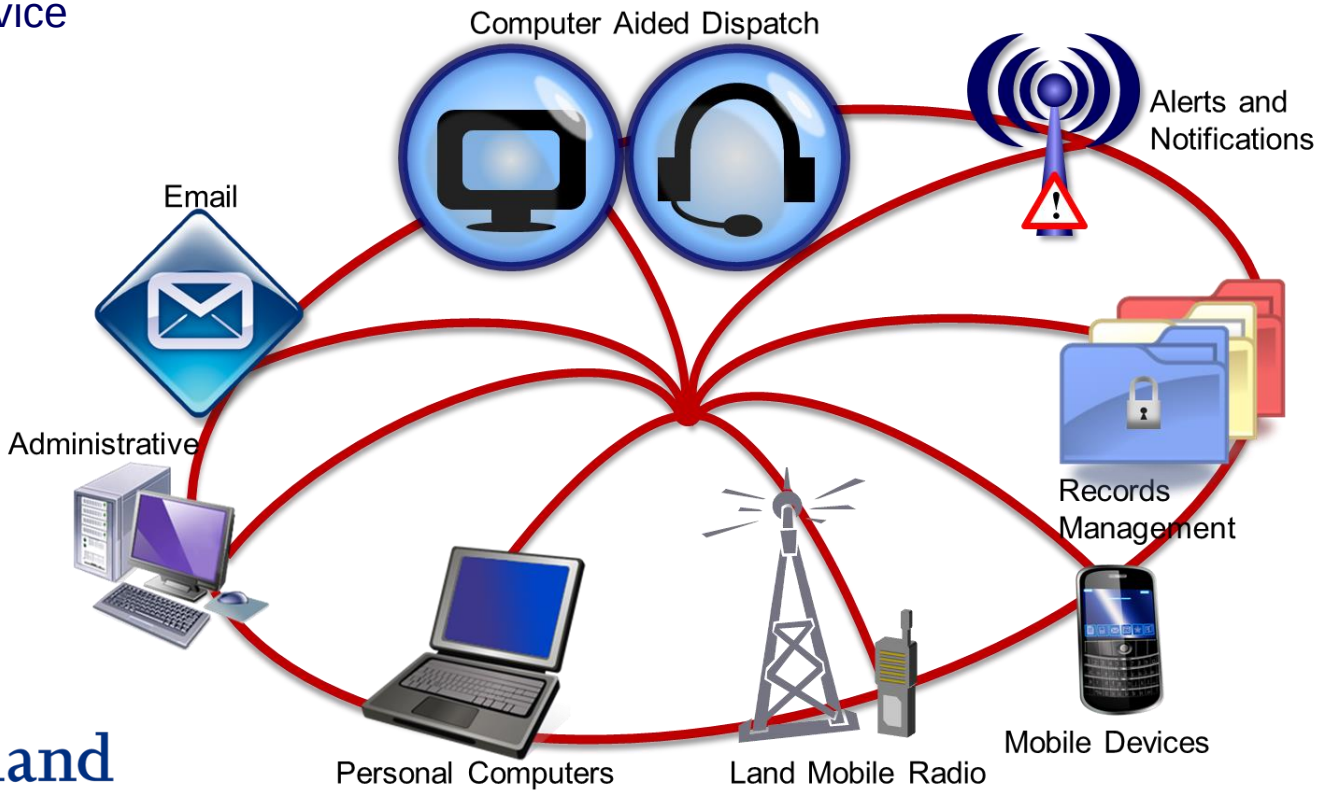
- NG 911 systems rely upon IP-based technologies to enable diverse multi-media, location-based services, and routing benefits
- Reliance on IP exposes NG 911 PSAP systems to a new, online threat environment, creating a heightened vulnerability to attacks through IP networks
- Communication through NG 911 may hide malicious threats (e.g. viruses can be embedded in texts, images, video and other files)
- NG 911 systems connect with other critical systems or devices; infecting one NG 911 system may impact other integrated systems (i.e., records management systems)
- Threat awareness and monitoring can enable NG 911 system capabilities within a more secure cyber environment
- Adoption of effective cybersecurity measures will help to ensure that PSAP mission-critical systems are secure and operational

Threats and Exploits to NG 911 Systems

Exploit	Description	Mitigation
Telephony Denial of Service (TDoS)	Preventing or delaying the ability to answer emergency calls by flooding the system with a volume of calls that exceeds the ability to service	• Do not pay or engage callers • Report all attacks to the FBI at www.ic3.gov • Collect time, date, originating phone number, traffic characteristics of TDoS attack • Contact telephone service provider for assistance
Distributed Denial of Service (DDoS)	Placing high processing demands on the system's server or network rendering it unavailable	• Monitor system traffic to increase awareness and identify an attack • Report anomalies to managers and technical staff per policies
Phishing/ Spearphishing	Sending emails that appear to come from a legitimate source such as a bank, credit card company, tricking recipient into providing sensitive personal information	Do not provide personal information such as social security, bank account numbers, user name or passwords in response to an email
Social Engineering	An attempt to trick someone into revealing information that can be used to attack systems or networks.	Do not give login credentials to unverified individuals
Identity Theft	Use of personal information of other persons, may occur as a result of phishing, social engineering, or illicit monitoring	• Do not allow "shoulder surfing" • Use unique passwords for different systems and sites • Change passwords frequently • Do not loan your log in information to others

Cascading Vulnerabilities

- A successful cyber attack on one system may endanger all connected systems, through—
  - Common login/ credentials
  - Unsecure network
  - Denial of service



Homeland Security

Potential Impact of Attack on Public Safety

Technology & Information	Types of Attacks	Impact	Consequences
Computer Aided Dispatch (CAD)/911	Denial of Service (DOS)/TDOS; Malware, viruses, Trojans	Disruption of emergency services/communication	Severe risk to both public and officer safety; loss of public confidence
Land Mobile Radio (LMR)	DOS, Malware, jamming, physical attack on transmitters, loss, or damage due to vandalism or forces of nature	Disruption or loss of communications	Severe risk to both public and first responder safety
Records Management System (RMS)	Malware, Trojan, keystroke logger; physical intrusion/ loss or theft	Loss or distortion of information/evidence; privacy and HIPPA	Threat to safety of individuals, responders, informants, etc. degradation of evidence; case/judicial impact; loss of public trust
Investigative Databases	Malware, Trojan, keystroke logger, false credentialing	Loss or distortion of information/evidence	Threat to safety of individuals, officers, informants, etc. degradation of evidence; case/judicial impact; privacy violations; loss of public trust
Wireless Mobile Devices	Malware, virus, intrusion, loss or theft	Loss of communications and confidential information; disruption of duties	Threat to responder and public safety; breach of privacy
Public Safety Information (digital and hard copy)	Loss or theft by both electronic and physical means	PII-type info and confidential info released	Significant potential liability, potential violation of statutes, responder and public safety diminished. Severe risk of public trust

Cybersecurity Risk Mitigation

- To prepare your agency to operate securely in a cyber environment, establish a Cybersecurity Risk Mitigation Strategy
- A Cybersecurity Risk Mitigation Strategy will facilitate clear and consistent understanding, across your agency, on—
  - **Governance**: Set expectations for periodic risk/vulnerability assessments and audits
  - **Policy**: Identify security policies, goals and objectives to address risks
  - **Plans**: Develop a security incident alert/response plan and a business continuity/disaster management plan
  - **Budget**: Establish security as a part of the budget process
  - **Roles and Responsibilities**: Designate a security risk manager and clarify responsibilities for staff
  - **Training**: Establish cybersecurity training and awareness plan

Cybersecurity Governance and Planning – Keys to Success

- Start by assessing which functions and leaders are involved in your cybersecurity efforts…expand if needed
- Establish and kick-off a planning effort
- Inventory, understand and identify risks of systems that connect to the internet and information (e.g., RMS, CAD, personally-owned mobile devices, PII information)
- Identify the risks to which your agency is susceptible, including specific systems/information that are at risk and the threats they face
- Focus on policies and ***SOPs to prevent intrusions*** and ***respond*** once they occur
- ***Establish a process to train employees*** on cybersecurity requirements and what to do in the event of an intrusion, data breach, or unauthorized access
- A comprehensive Cybersecurity Plan is an important step for your agency to establish the foundation, policies, and response procedures to better prevent, detect, respond to, and recover from, a cyber incident

Establishing Cybersecurity Policies

- *The creation of a security policy is the first step in any effective attempt at implementing a security program. A security policy is a clearly documented statement of organizational goals and intentions for security, particularly upper management's commitment to security.* NENA NG-911 Standard (NG – SEC)
- When establishing a cybersecurity policy, consider how users should appropriately access PSAP systems (i.e., CAD, email). Effective cybersecurity policies address—
  - **User Identification & Authentication**: Strength of passwords, multi-factor identification, password management and recovery
  - **Devices**: Acceptable devices and use policies, clear personal device policies
  - **Connectivity**: Wired, Wi-Fi, Bluetooth security practices
  - **Access**: To resources, systems, databases, and applications
  - **Hosting**: Dedicated/registered domain name (DNS) for emergency communications, commercial email, onsite or offsite "cloud" systems
  - **Data Management**: Use of personal storage devices and use of peer-to-peer programs
  - **Encryption**: Securing communications for sensitive information in accord with U.S. law

Cyber Security Resources

- The Next Generation of Security for NG9-1-1 SYSTEMS; The Challenge of Securing Public Safety Agencies; A white paper from L.R. Kimball January, 2010 www.lrkimball.com/cybersecurity accessed 2/22/2014
- NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) NENA 75-001, Version 1, February 6, 2010 www.nena.org
- NENA Next Generation 9-1-1 (NG-SEC) Audit Checklist NENA 75-502 Version 1 December 14, 2011 www.nena.org
- National Institute of Standards and Technology (NIST): http://www.nist.gov
- NIST Framework for Improving Critical Infrastructure Cybersecurity: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
- NENA Best Practices for TDOS http://www.nena.org/news/120618/Best-Practices-Checklist-for-Denial-of-Service-Attacks-Against-9-1-1-Centers.htm
- NENA 04-503, NENA Technical Information Document Network/System Access Security Issue 1, December 1, 2005 www.nena.org
- The NIST Glossary of Key Information Security Terms, NISTIR 7298 Revision 2 Requirements and Transition Document

GIS in NG9-1-1

- Fully integrated into NG911, responsible for call routing
- Provide sufficient graphical information to locate the caller
- Provide supporting geographic information as needed for Incident Command, field decision making
- Civic (123 Main St) or long-lat (x-y) used to route call
- On the fly response changes possible
- No separate MSAG and GIS databases
- ***Location, rather than telephone number is used for routing in Next Gen 9-1-1***

GIS in NG9-1-1

- GIS plays crucial role in NG9-1-1 call routing -ECRF
- Routing database is GIS data centric
- Accuracy of GIS data is paramount
- Shared data –coordination
- 9-1-1 authority is responsible for the data
- Location is delivered with call
- Location is pre-validated using GIS data -LVF

GIS in NG911

- The GIS data used in Next-Gen goes by names like LVF* and ECRF***. They're called 'Functions', but are GIS databases.
- Location Validation Function
- Emergency Call Routing Function
- These database will have a standard schema (see NENA 08-003), that will be the same nationwide for exchange.

GIS in NG9-1-1

- Next Generation 9-1-1 **requires** GIS Data
- Wide range of needs for address data statewide
- Build to the highest level requirements (9-1-1), able to support lower requirements.
- Support 9-1-1 dispatch
- Be available for other widespread uses
- Support high-quality geocoding
- Stripped of personal information

GIS LAYERS FOR NG911

- Road Centerline (required)
- Emergency Service Agency Location (required)
- Emergency Service Agency Boundary (required)
- Cell Site Locations/ Coverage Areas (required)
- County Boundaries (required)
- Emergency Service Zones Boundary (required)
- Municipal Boundaries (required)
- Railroads (optional)
- Hydrology (optional)
- Road Mile Markers (optional)
- Site/Structures (optional)
- Imagery (optional)

Next-Gen changes the use of GIS in 9-1-1

- Additional layers that are, or will become quite useful:
  - Address points or parcels, if you don't already have them
  - Building footprints
  - Apartment complexes – with detail
  - Business location, with detail such as hazmat information
  - Mile markers, intersections (not just roads), place names
  - All kinds of imagery, plus LIDAR, building photos, floor plans, etc.

Homeland Security

GIS data used for call routing

- Accuracy of data will determine correct routing of call
- GIS road centerlines, address points and jurisdictional boundaries all become focus of emergency routing databases
- What can you be doing to prepare GIS data?Synchronize GIS with MSAG and ALINENA 71-501, Version 1.1, September 8, 2009
- Completed address points layers
- Edge-matching boundaries, centerlines

Current NG911 Activities

Homeland Security

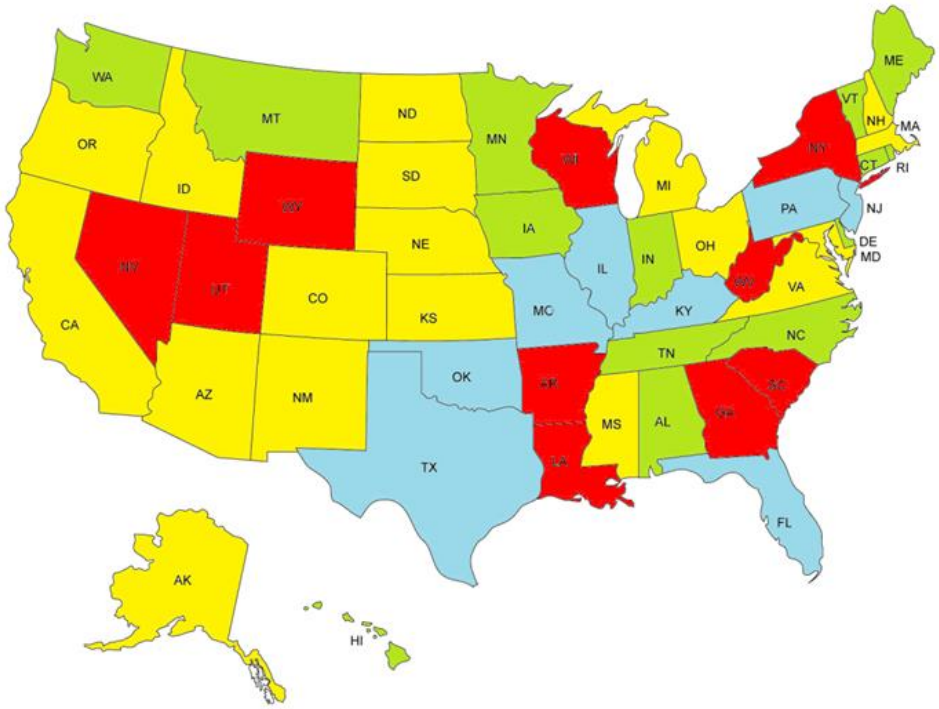
OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

Status of State Planning & Preparation

- Approximately thirty states have developed NG911 Master Plans or Strategic Plans which define the technology, operations, governance associated with the transition to an IP-based NG911 capable system
- Twenty-five states have begun deploying aspects of an IP-based NG911 system
  - The number is growing
  - Many are implementing statewide IP networks
  - In some cases, regional systems are leading the states
- The following slides provide a small sampling of different implementation approaches; with additional detail for Indiana and Maryland

A Look at NG Across The Country



GREEN — States are in some stage of implementation of a statewide ESINet (Emergency Services IP Network) or NG9-1-1 system

YELLOW — States are in some stage of Planning for the migration to a NG9-1-1 system

BLUE — States are in some stage of NG9-1-1 implementation at regional levels in the state (not a statewide initiative)

RED — States have not made significant progress towards NG9-1-1

Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

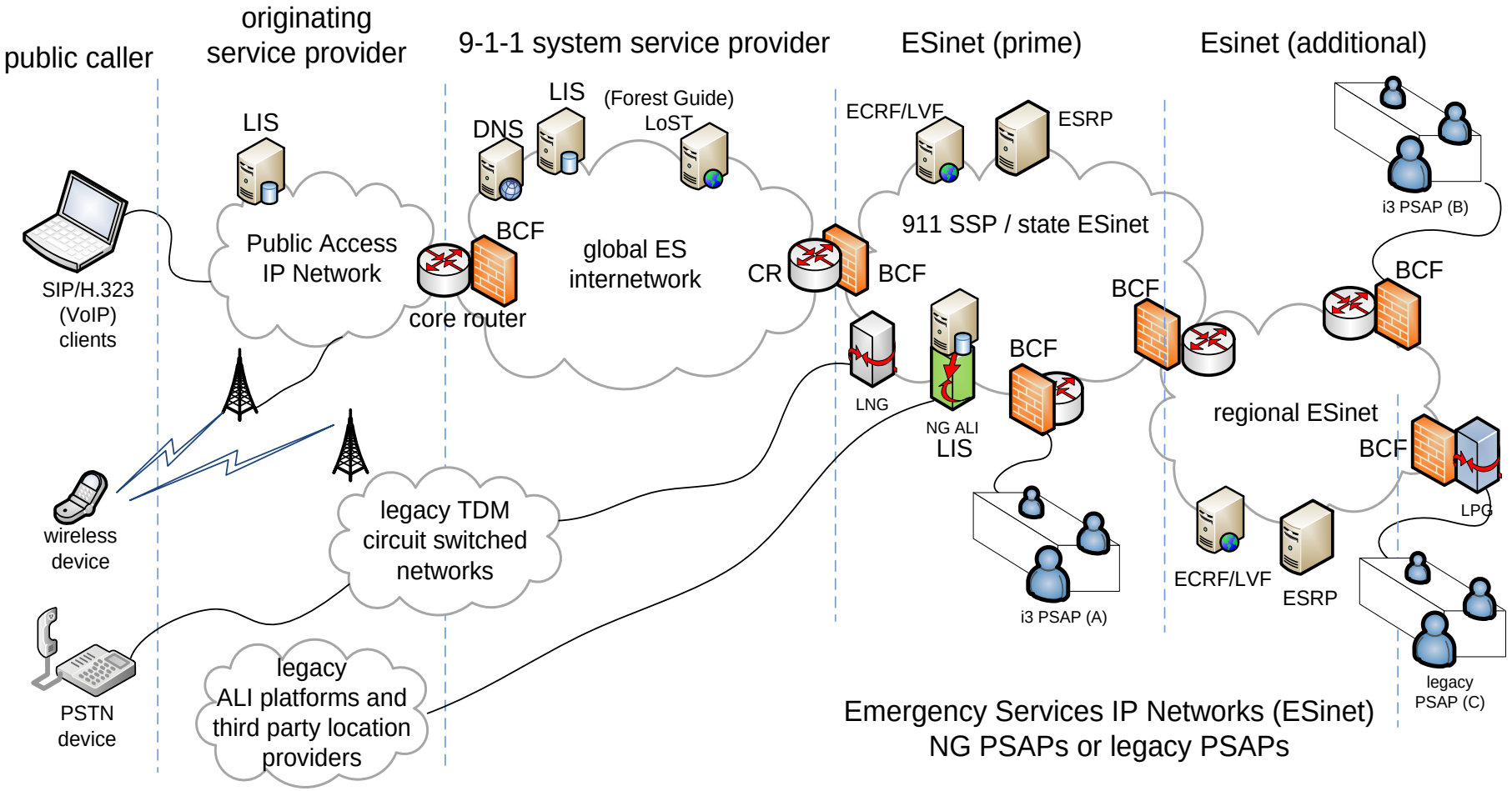
The Mid-Atlantic and Other Projects of Note

State	Activity	Notes
Delaware	NG Planning ESInet	Planning/consensus building – i3 Network close to implementing a three PSAP solution. Recently announced award of an ESInet and i3 service provider.
Indiana	ESInet	NG9-1-1 implementation in progress at state level. IN9-1-1, text, direct IP connections are operational.
Maryland	NG Planning, CPE	State board in place, exploring remote hosting phone equipment. NG pilot project planned for State Police. Worked with a consultant.
Massachusetts	NG Planning	NG9-1-1 prep activity at state level. Recently released an RFR seeking turnkey NG9-1-1 integrated system
New Jersey	NG Planning	ICTAP Workshop, and planning/discussion underway
New York		NG9-1-1 implementation in progress at sub-state Level. No real state level agency with authority to implement.
Pennsylvania	ESInet	NG9-1-1 prep activity at sub-state level. Regional ESInet and CPE projects are being funded.
Virginia	Leg/Reg	Four pilot projects completed. NENA i3 solution. Some regional activity. Recently completed a NG911 Study
TN		

Indiana – IN911

- The Indiana NG911 system is implemented and operated by a service contractor using the Indiana Fiber Network, IN911, and leased facilities which provide core ESInet and i3 process capability
- So far, the system has focused on wireless calls because at inception, the only purview of the Indiana 911 Board was wireless
- There are two wireless service aggregation points
- PSAP CPE is a mix of premises and remote-hosted
- Currently 36 PSAPs are hosted
- Some wireline calls now traverse IN911, but only for hosted PSAPs
- In 2008, the state mandated no more than 2 PSAPs per county by 2014
  - Only 5 counties remain

IN911 – TDM - i3 Diagram



This diagram represents a basic and TDM transitional NG9-1-1 architecture.

The objective is to demonstrate how a hiearchical distribution of functional elements facilitate a public caller's ability to be routed to the proper PSAP.

Homeland Security

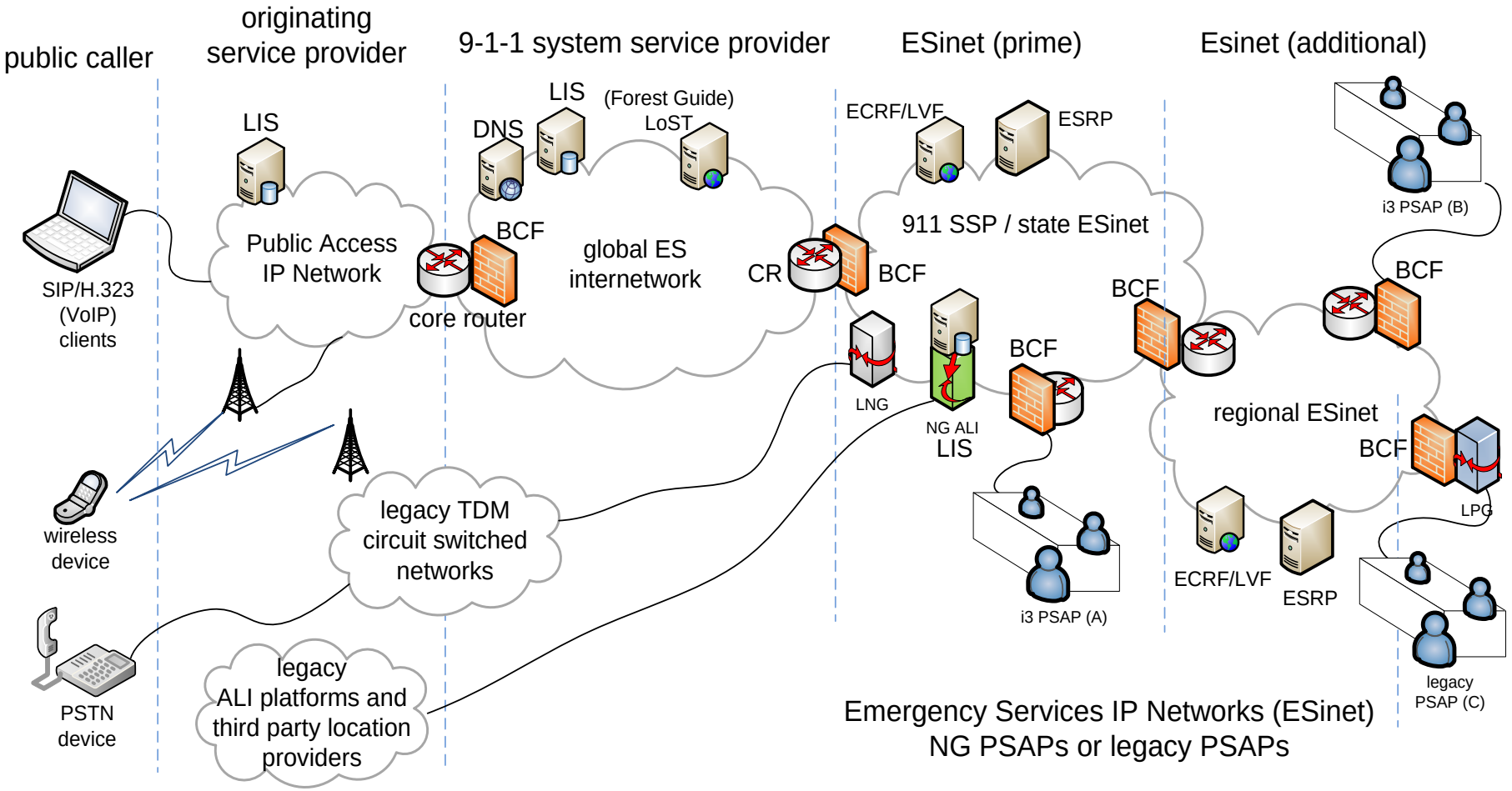
OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

Tennessee

- The Tennesee NG911 system uses the NetTN network, a state-wide all-digital network
- There are two fully-redundant network control centers which route all NG9-1-1 calls
- Initial deployment focused on wireless carriers
- There are four wireless service aggregation points
- Each wireless carrier must connect to at least two wireless service aggregation points
- Network Operations Center (NOC) established
- Text to 9-1-1 pilot with AT&T – SMS over IP
- NG9-1-1 project under budget every year since beginning of deployment

Tennessee TDM - i3 Diagram



This diagram represents a basic and TDM transitional NG9-1-1 architecture.

The objective is to demonstrate how a hiearchical distribution of functional elements facilitate a public caller's ability to be routed to the proper PSAP.

Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

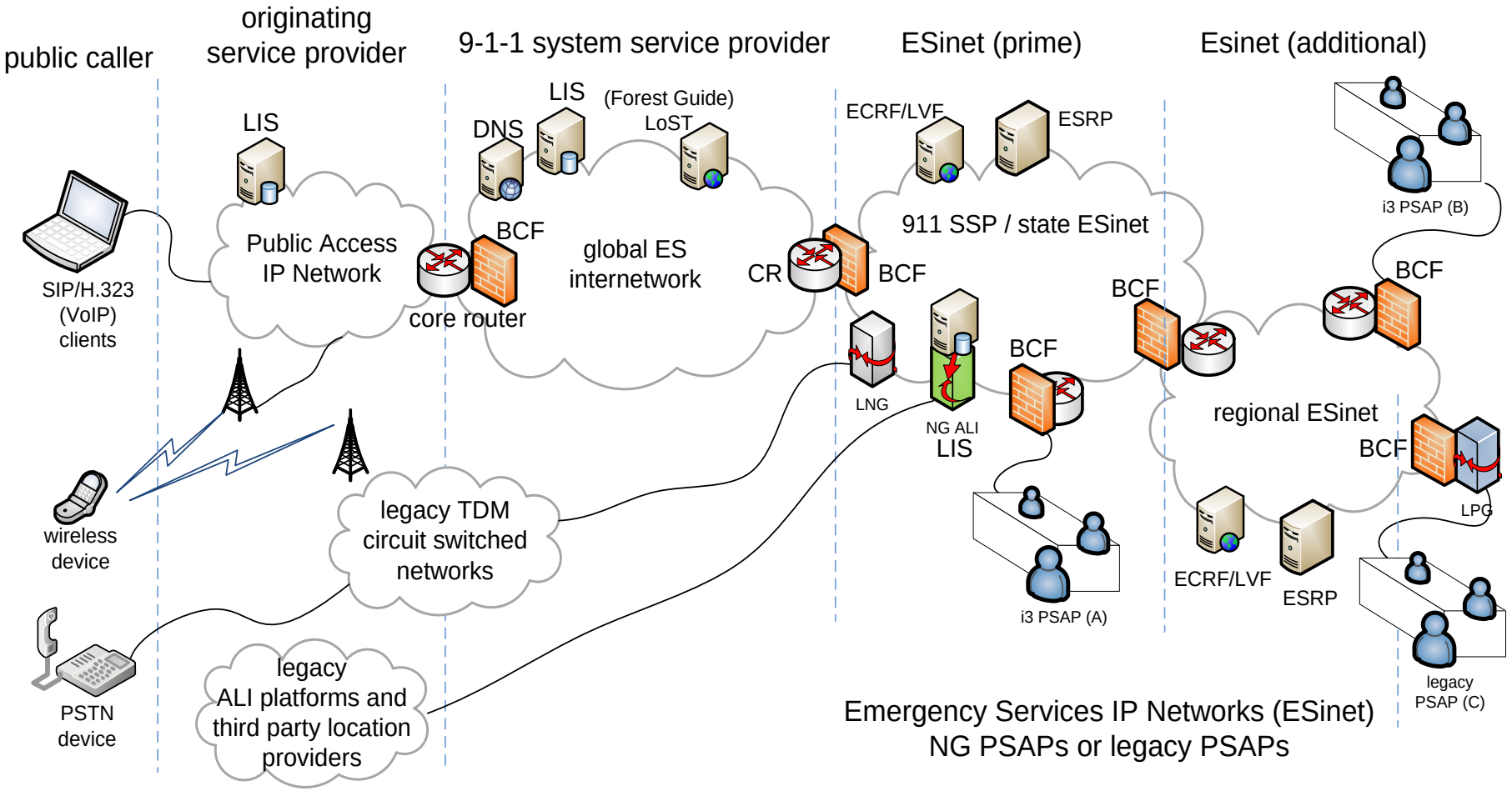
Massachusetts Statewide System Replacement - 2014

- State wide E911 call taking system provided under contract by Verizon
- Equipment end of life,
- Verizon not interested in renewing contract
- Put RFP out for new system
- Sought CPE, ESInet, i3 functions, TDM to NG transition, Training, Implementation, Testing, Operation, Maintenance, Monitoring, Management and Daily Operations/Support
- Awarded new contract in August of 2014 to a team led by General Dynamics Information Technology Division (GDIT)
- Synergem
- Emergency CallWorks
- Windstream

MA Scope and Size

- The State 911 Department currently provides services and equipment for approximately two hundred fifty-four (254) PSAPs throughout the Commonwealth, as well as for approximately one hundred four (104) limited secondary PSAPs, three (3) secondary PSAPs, four (4) training centers, and one (1) mobile PSAP
- There are currently approximately 6,000 certified enhanced 911 telecommunicators throughout the Commonwealth

What MA Asked For – TDM - i3 Diagram



This diagram represents a basic and TDM transitional NG9-1-1 architecture.

The objective is to demonstrate how a hiearchical distribution of functional elements facilitate a public caller's ability to be routed to the proper PSAP.

Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

NG911 Next Steps

Early start options can be secured by taking any of the following steps

- Begin the provisioning of a secure IP network
  - Expand IP network built with DHS grant funding
- Provide a GIS system with detail and layers necessary for NG911
- Begin the installation of IP-based CPE in the PSAPs
  - Encourage common sourcing
- Conduct proof of concept pilot demonstrations

Useful References

1. NG911 Transition Plan Considerations (JID), National Emergency Number Association (NENA), NENA 77-501 v1, February 24, 2011
2. NG911 System and PSAP Operational Features and Capabilities Requirements, NENA 57-750, v1 (Draft), March 2, 2011
3. Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3, NENA 08-003 v1, June 14, 2011
4. Next Generation 911 Transition Policy Implementation Handbook, Application of the Implementation Checklist, NENA, June 2011
5. i3 Technical Requirements Document, NENA 08-751, Issue 1, September 28, 2006
6. NG911 System Initiative, NG911 Preliminary Transition Plan, v1.0, USDOT April 2008
7. NENA Master Glossary of 911 Terminology, NENA 00-001 v16, August 22, 2011

Many more NENA standards and companion documents at www.nena.org

NG911 Resources

- National Telecommunications and Information Administration: http://www.ntia.doc.gov/
- DHS – Office of Emergency Communications: http://www.dhs.gov/xabout/structure/gc_1189774174005.shtm
- DOT – NG911 Initiative: http://www.its.dot.gov/ng911/index.htm
- DOT – National 911 Program: http://911.gov
- Industry Council for Emergency Response Technologies (iCERT): http://www.theindustrycouncil.org/index.cfm
- NG911 Institute: http://www.e911institute.org/
- Association of Public Safety Communication Officials: http://www.apco911.org/
- National Academies of Emergency Dispatch: http://www.emergencydispatch.org/
- National Association of State Nine-One-One Administrators: http://www.nasna911.org/index.php
- National Emergency Number Association: http://www.nena.org/
- NENA Master Glossary of 911 Terminology (00-001 V16): http://www.nena.org/?page=Glossary
- Next Generation Safety Consortium: http://www.nextgensafety.org/
- The National 911 Education Program: http://wwww.know911.org

NG911 Affiliated Organizations

- FCC: Federal Communications Commission
  - PSHSB: Public Safety Homeland Security Bureau
  - NRIC: Network Reliability and Interoperability Council
- DOT: U.S. Department of Transportation
  - NHTSA: National Highway Traffic Safety Administration
  - RITA: Research and Innovative Technology Administration
  - 911.gov: National 911 Program
- DHS: Department of Homeland Security
  - OEC: Office of Emergency Communications
- NENA: National Emergency Number Association
- APCO: Association of Public-Safety Communications Officials
- NASNA: National Association of State Nine-One-One Administrators
- IETF: Internet Engineering Task Force
- ATIS: Alliance for Telecommunications Industry Solutions
  - ESIF: Emergency Services Interconnection Forum

Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

QUESTIONS?

BACKUP

The Federal Government and NG911

Homeland Security

OEC/ICTAP

Office of Emergency Communications / Interoperable Communications Technical Assistance Program

FCC Recommendations to Congress

In February 2013, the FCC delivered their NG911 report and recommendations to Congress, provided in response to a provision in the Middle Class Tax Relief and Job Creation Act of 2012. The report focuses on three general recommendations to Congress—

- First, create incentives for the states to become early NG911 adopters
  - Accelerates NG911 migration in those states
  - Provides basis for easier transition in other states
- Second, promote the development of location technologies
  - To support response regardless of the network or the device used by the caller
- Third, assist in the identification of legacy state regulations that impede NG911 utilization
  - Includes incentives for states to modernize their laws and regulations
  - Both (1) liability and (2) impediments to implementation of new technology

FCC Recommendations to Congress (cont.)

- Specific recommendations
  - Create mechanisms such as challenge grants and other competitive funding programs to incentivize states to become NG911 “early adopters”
  - Encourage states to empower 911 boards (or similar) to provide guidance
  - Address instances where states lack authority to regulate elements of NG911 service
  - Require common standards for ESInet interfaces with other public safety entities
  - Include liability protection in any Federal laws related to NG911
  - Enact legislation requiring network access providers to support location determination
  - Ensure security standards and best practices for NG911 network security, including funding a credentialing authority
  - Encourage states to modify regulations that impede implementation of next generation technology
  - Promote consolidated regional NG911 call centers through incentives such as preferences for grants
- Recommends information tools for tracking NG911 progress
  - Upgrade the National Master PSAP Registry and the National 911 Profile Database to include information on NG911 implementation
  - Support the development of web-based data filing capability
  - Provide tools for automatic report generation

This FCC report is available at:
http://www.fcc.gov/document/legal-and-regulatory-framework-ng911-services-report-congress

Regulations that Impact NG911

Federal Communications Commission (FCC)

- Report to Congress on the Legal & Regulatory Framework for NG911 Services
  - Identifies potential steps for Congress to take to create a legal and regulatory environment that will assist states, PSAPs, service providers and other stakeholders in accelerating the nationwide transition from legacy 911 to NG911.
- PS Docket No. 13-75 – NPRM: Improving 911 Reliability
  - Comments on approaches to ensure the reliability and resiliency of the communications infrastructure necessary to ensure continued availability of the Nation's 911 system, particularly during times of major disaster
- PS Docket No. 11-153 – Facilitating the Deployment of Text-to 911 and Other Next Generation Applications
  - Amends the Commission's text-to-911 "bounce-back" requirement as it applies to Commercial Mobile Radio Service (CMRS) providers when consumers are roaming

Federal Legislation Impacting NG911

- Wireless Communications and Public Safety Act of 1999 - Pub. Law 106-81
  - Promote and enhance public safety through use of 911 as the universal emergency assistance number
  - Further deployment of wireless 911 service
  - Support of States in upgrading 911 capabilities and related functions
  - Encouragement of construction and operation of seamless, ubiquitous, and reliable networks for personal wireless services, and for other purposes
- ENHANCE 911 Act of 2004 - Pub. Law 108-494
  - Established National E911 Implementation and Coordination Office (ICO)
  - Charged the ICO (now the National 911 Program) with:
    - Coordinating the implementation of 911 and E911 at the Federal, State, and local levels
    - Administering a Federal PSAP grant program authorized to provide up to $250 million in grants per years
    - Ensuring that funds collected on telecommunications bills for enhancing emergency 911 services are used only for the purposes for which the funds are being collected

Federal Legislation Impacting NG911

- Implementing Recommendations of the 9/11 Commission Act of 2007 - Pub. Law 110-53
  - Makes $43.5 million available for PSAP grants authorized by the ENHANCE 911 Act of 2004 after 180 day rulemaking to determine criteria to receive grants (Title XXIII)
  - Authorizes $950 million per year for fiscal years 2008-2012 for a State Homeland Security Grant Program (Title I, Sec. 2004) and makes clear that such funds can be utilized for "supporting Public Safety Answering Points" (Title I, Sec. 2008)
  - Authorizes nearly $3.5 billion in Emergency Management Performance Grants which can be used for the construction of Emergency Operations Centers (Title II)
  - Establishes an Interoperable Emergency Communications Grant Program and authorizes $1.6 billion in grant funding for fiscal years 2009-2012 (Title III)
- New and Emerging Technologies (NET) 911 Improvement Act of 2008 - Pub. Law 110-283
  - Promotes and enhances public safety by facilitating the rapid deployment of IP-enabled 911 and E–911 services
  - Encourages the Nation's transition to a national IP-enabled emergency network
  - Improves 911 and E–911 access to those with disabilities

Middle Class Tax Relief and Job Creation Act, 2012

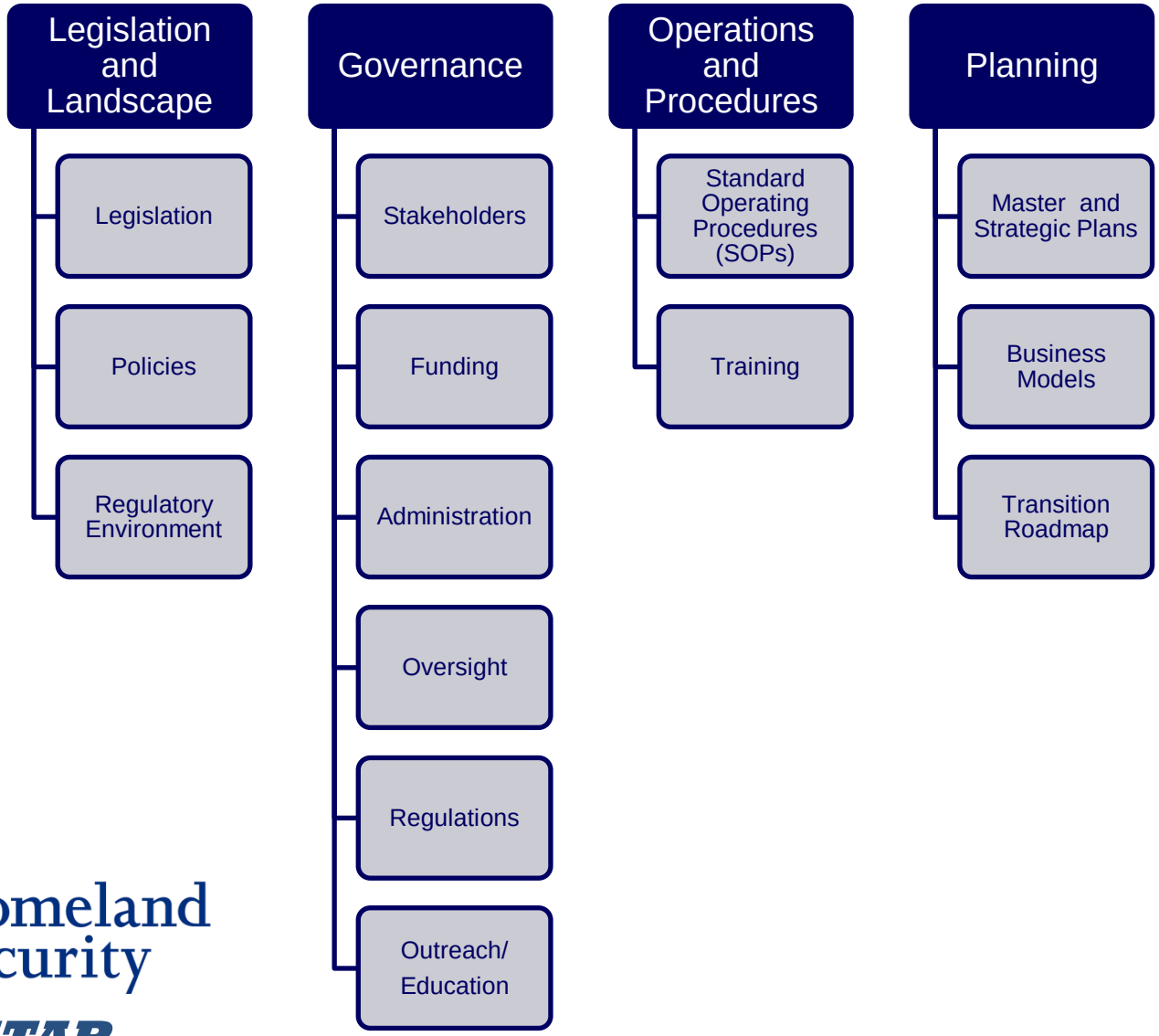
- The Middle Class Tax Relief and Job Creation Act of 2012
  - Signed into law in February 2012
  - Provides $115 million for NG911 and begins a multi-year process of building a public safety broadband network that must interconnect with NG911 systems
  - Requires studies examining current 911 fees and the costs associated with NG911 that will allow Congress to address system development, deployment, and maintenance funding issues
  - Funds will be provided from the auction of commercial spectrum and will be distributed in descending order of priority
  - Funds are available until Sept. 30, 2022, after which they revert to the Treasury for deficit reduction

Title	Amount	Description
Network Construction Fund	$7 Billion	From spectrum auctions for construction, operations/maintenance/etc. Up to $2B for FirstNet startup costs
State and Local Implementation	$135 Million	Grants to assist with planning & implementation. Requires 20% match coordinated through single agency/body.
NIST Public Safety Research and Development	$100 Million	Funding for NIST to support research and development of standards, technologies, and applications to advance wireless public safety communications
Deficit Reduction	$20.4 Billion	Returned to the U.S Treasury for deficit reduction
NG911	**$115 Million**	**To support NHTSA grant program on NG911. Provided only after deficit reduction target is met.**
Additional NIST R&D	$200 Million	Provided only after deficit reduction target is met.

NG911 and NPSBN Integration

- The Middle Class Tax Relief and Job Creation Act of 2012 created the First Responder Network Authority (FirstNet) and the Nationwide Public Safety Broadband Network (NPSBN)
- FirstNet is an independent authority within the National Telecommunications and Information Administration (NTIA) responsible for providing emergency responders with the first high-speed, nationwide network dedicated to public safety
- NG911 and FirstNet are ideally suited to work together:
  - Both NG911 and NPSBN are IP-based systems with the goal of transmitting voice, video, pictures, and data
  - Integrating the networks provide the ability for seamless transfer of data from the community to the 911 call takers via the NG911 system and then from the 911 call taker to emergency responders via NPSBN
- However, there are some technical obstacles that may impede integration efforts including:
  - A suitable protocol for system interconnection must be proven reliable
  - Technical concerns including prioritization, quality of service, authentication, and roaming charge tracking must be addressed
  - LTE support for public safety wireless features (e.g., direct mode & group calls)
- In July 2013, FirstNet released 10 requests for information in an effort to determine the most effective network design approach. One of these RFIs (Network Service Platform) discusses critical applications and services required by the network manager and end users including NG911

Strategic Planning Considerations



Interim (Pre-NG9-1-1) Text-to-911

In December 2013, the FCC adopted a Further Notice of Proposed Rulemaking (FNPRM) to facilitate deployment of Text-to-911

- Summarizes cost, schedule, and technical issues
- Identifies potential solutions along with impact on carriers, vendors, and PSAPs
- Builds on voluntary commitment by the four largest wireless carriers to make Text-to-911 available by May 2014

  (Now!)

Final comments received in March 2014

SMS vs. MMS vs. MMES

- What is the difference?
  - *SMS* – Short Message Service
  - *MMS* – Multi-Media Service
  - *MMES* – Multi-Media Emergency Service

- 3, 4, 5, 6 or 10 digit code
  - SMS to 9-1-1 is also known as 3-digit short code

Length of Message

- There MAY not be a limit to the length of a message sent by the Texter, but the message may break into parts of 160 characters each when received at the PSAP.
  - If a message is lengthy (exceeding the 160 character limit), there is a potential for messages to arrive at the PSAP out of order.
  - Public education campaign should focus on the importance of a concise message.