# State of Wisconsin
# NG 9-1-1 Overview Workshop

May 2016

Homeland Security

**Provided By**
**Office of Emergency Communications (OEC)**

# Introductions

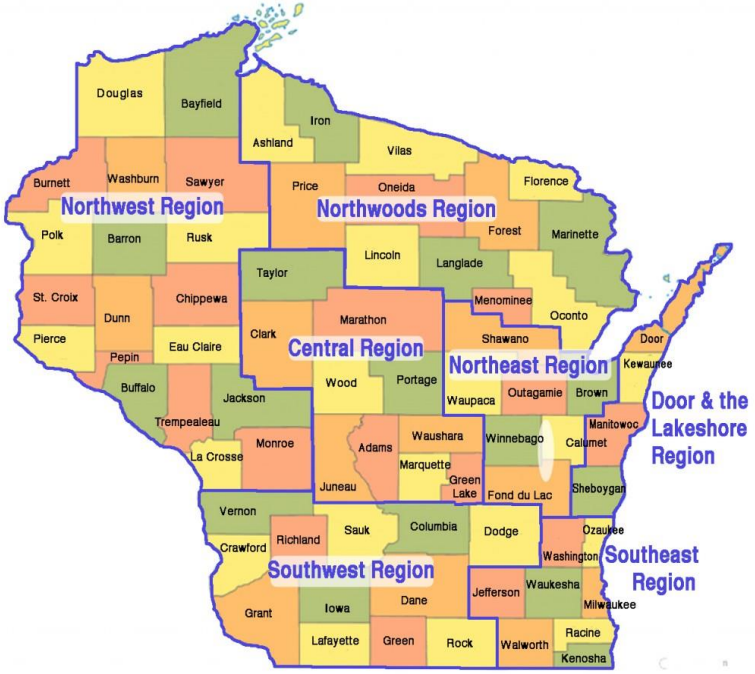
Nancy Dzoba – OEC/ICTAP
ndzoba@lafayettegroup.com

Chuck Spalding -OEC/ICTAP
cspalding@lafayettegroup.com

Jim Jarvis– OEC Region Coordinator
James.Jarvis@hq.dhs.gov

# Agenda

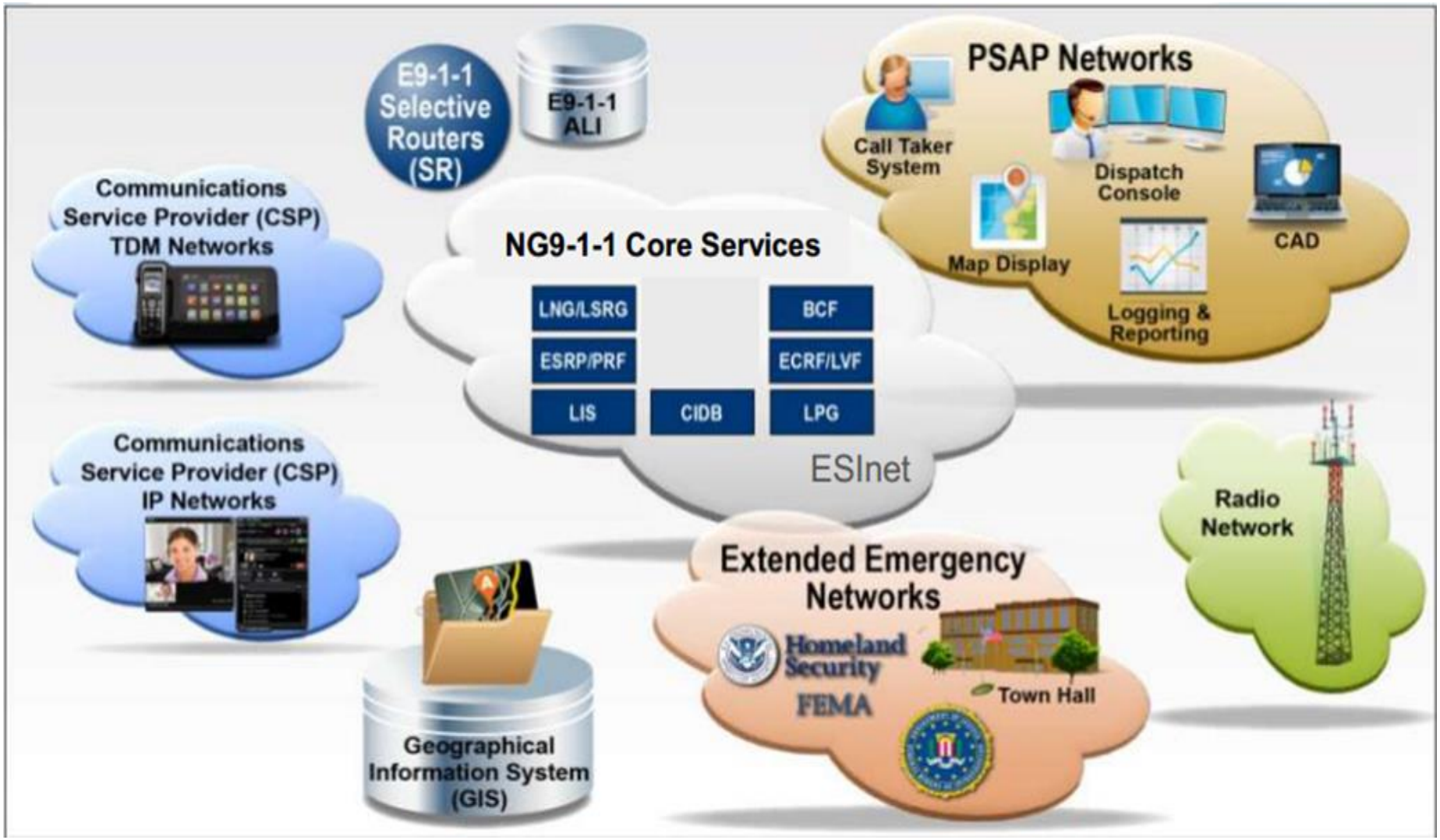
- **Why NG 9-1-1**
  - NG 9-1-1 Standards
  - 9-1-1 Today
- **NG9-1-1 Technology**
- **GIS & NG9-1-1**
- **Cybersecurity**



# What is NG9-1-1?

- New technology for routing and processing a 9-1-1 call
- Converts analog network to digital or internet protocol- (IP) based network
  - Allows for transmission of more mission critical information related to the 9-1-1 call
- Examples
  - Pictures and video
  - Crash or telemetry data
  - Real-time location information of emergency
- Provides first responders with more critical information for resolving emergency situations

# NG9-1-1 Ecosystem



# NG9-1-1 Improvements and Capabilities

## Expand PSAP Capabilities

- Transfer voice and data between all NG9-1-1 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

## Leverage Capability of Originating Devices

- Text-to-911
- Devices, such as sensors, generating data-only messages
- Photo and video transmission
- Telematics

## Interoperate with Other Emergency Systems and Entities

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

# 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

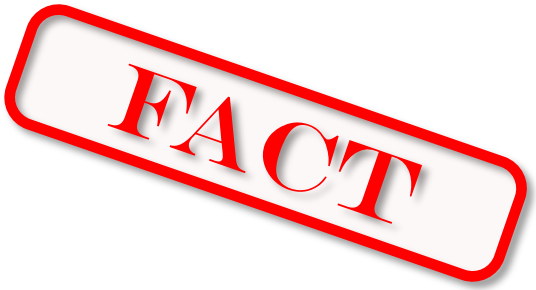
# Additional NG9-1-1 Benefits

- **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

# NG9-1-1 Myths and Facts

- **NG9-1-1 Myths**
  - The PSAP working environment will change radically overnight
  - Accurate location data is guaranteed
  - NG9-1-1 will immediately begin to save money
  - Harassing or malicious 911 calls will be eliminated

- **NG9-1-1 Facts**
  - NG9-1-1 replaces legacy circuit-switched technology with IP solutions
  - Establishes 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)



# NG9-1-1: Obstacles

- **Funding**
  - Primary reason NG9-1-1 activity varies across the country
  - Complicated by lack of understanding about the need for change
  - Inability to reserve funds for future capital costs in budget requests
  - Collected 9-1-1 fees used to pay unrelated costs
- **Lack of authority at state level agency**
  - Only 35 states have an authorized and staffed public safety function related to 9-1-1
- **Legislation**
  - Original legislation that established 9-1-1 has language which excludes new providers and/or technology in some states
- **Contractual obligations**
  - Bound by existing, long standing contractual obligations based on old technology
  - Termination costs can be prohibitive
  - Prevents some jurisdictions from moving beyond planning

# NG9-1-1 Technology

# 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

**Uses IP technology and standards**

- Packet-based rather than circuit switched
- Open systems design

**Location-centric**

- Caller location embedded in call delivery packets
- GIS vs. MSAG
- Location Information Server (LIS) vs. ALI

**E9-1-1 capabilities and much more**

Homeland Security

OEC/ICTAP

*Office of Emergency Communications / Interoperable Communications Technical Assistance Program*

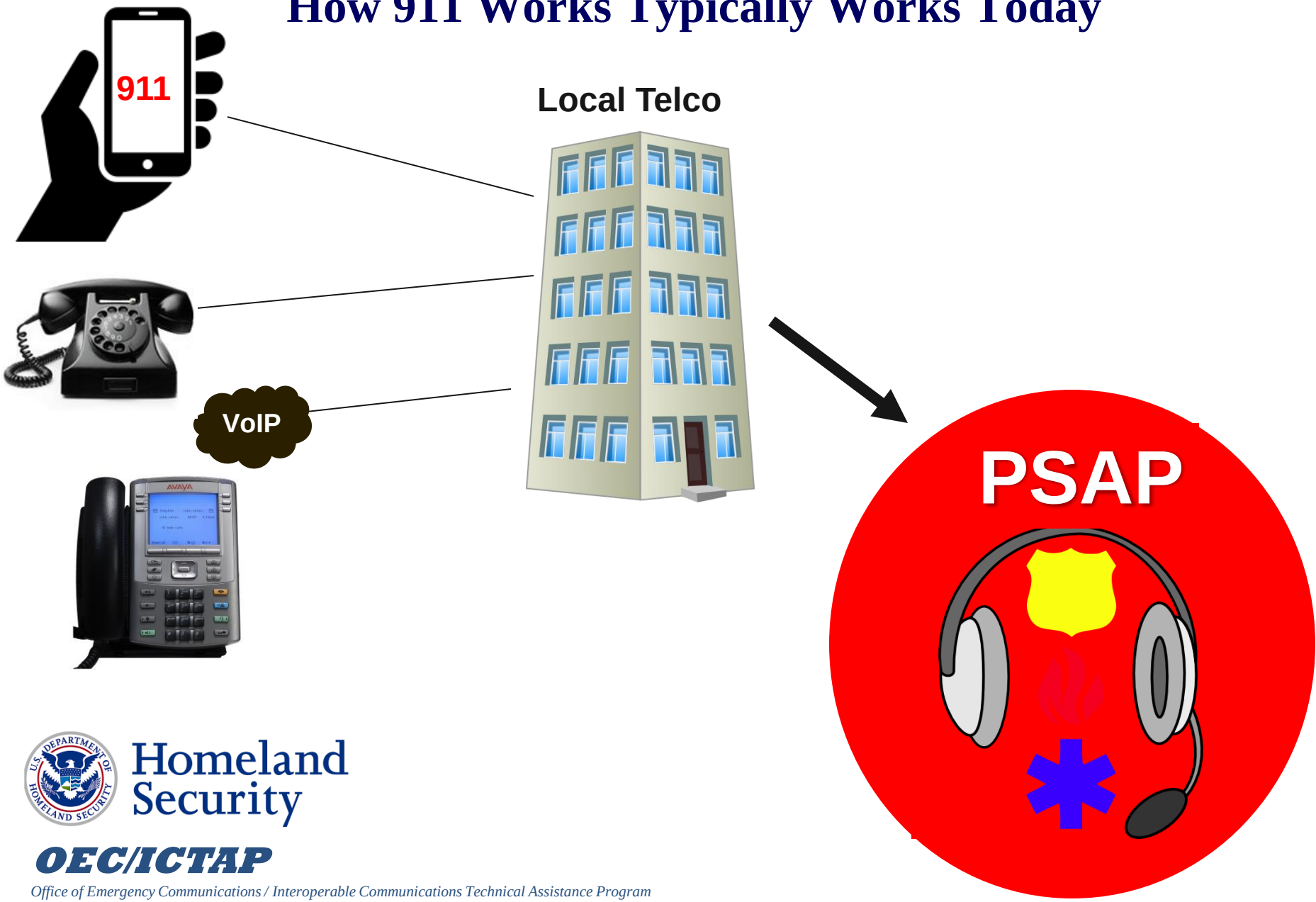
# NENA i3 Standard and ESInet

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

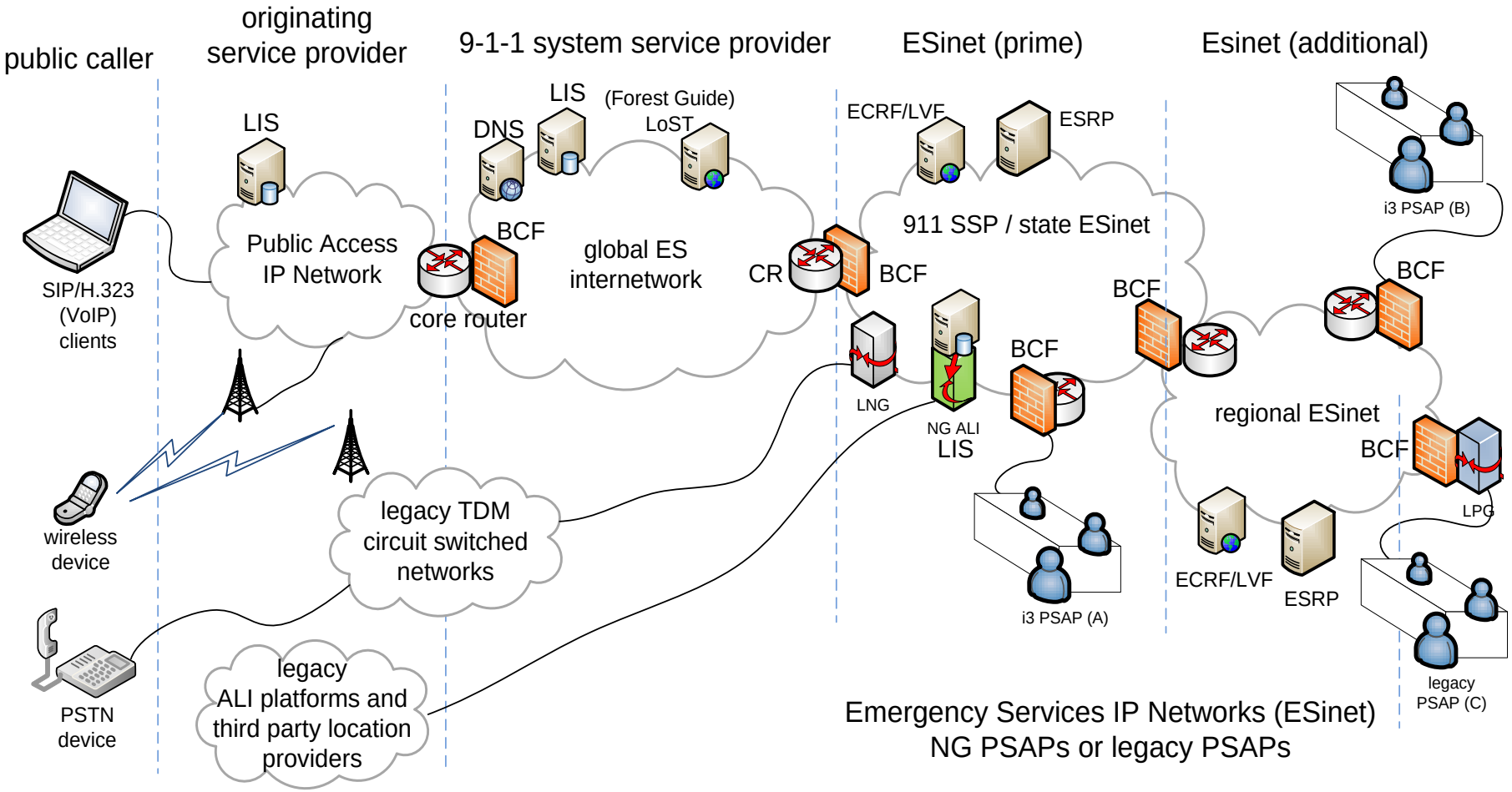
OEC/ICTAP

*Office of Emergency Communications / Interoperable Communications Technical Assistance Program*

# Evolution of 911

| | Today's E911 | NG9-1-1 |
|---|---|---|
| Networks | 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 | Limited | Very large, Broadband Data Bandwidth |
| Location Services | Wireless Routing Based on Cell Tower Sector | 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.

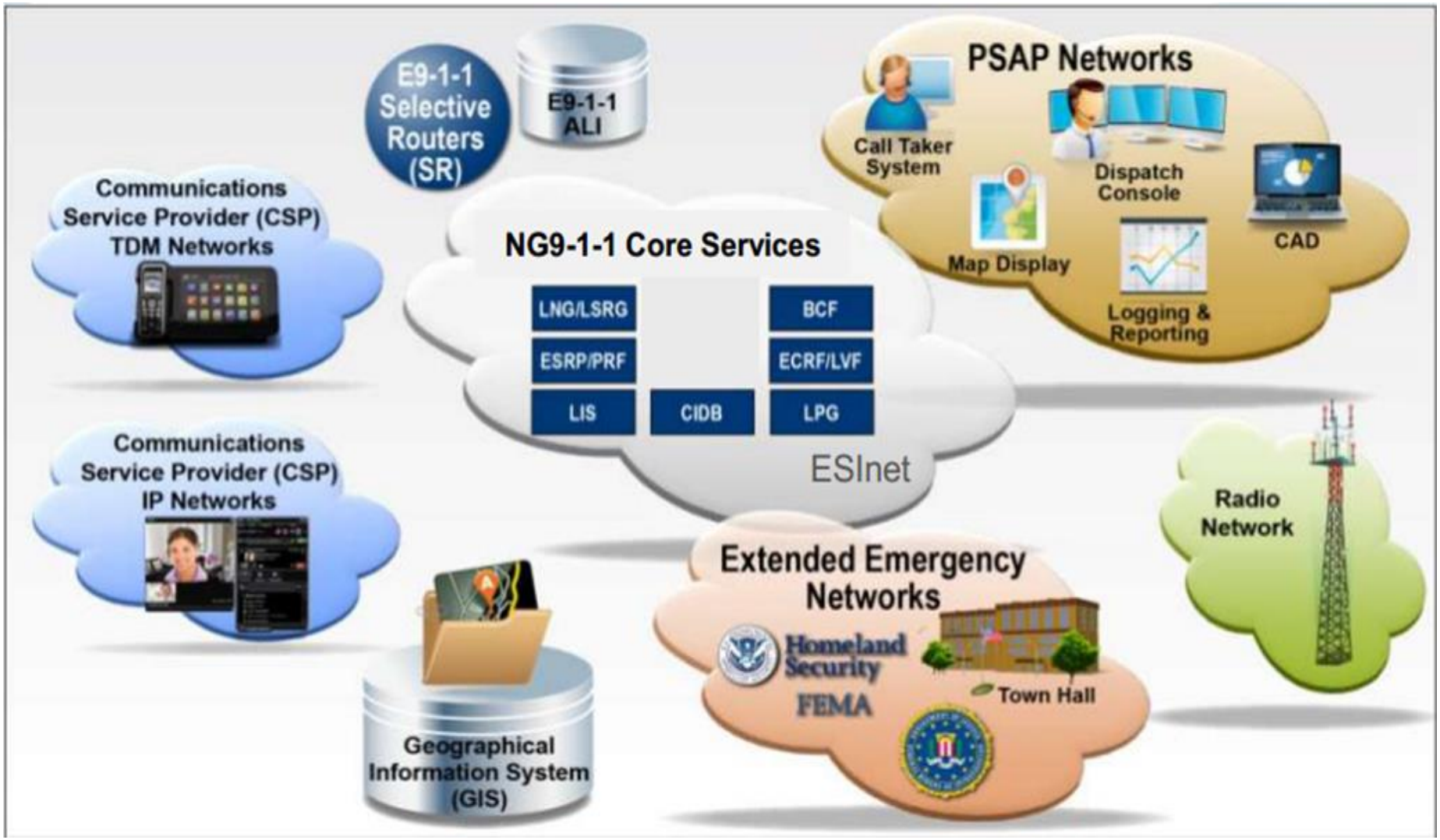
The objective is to demonstrate how a hiearchical distribution of functional elements facilitate a public caller's ability to be routed to the proper PSAP.

Homeland Security

OEC/ICTAP

*Office of Emergency Communications / Interoperable Communications Technical Assistance Program*

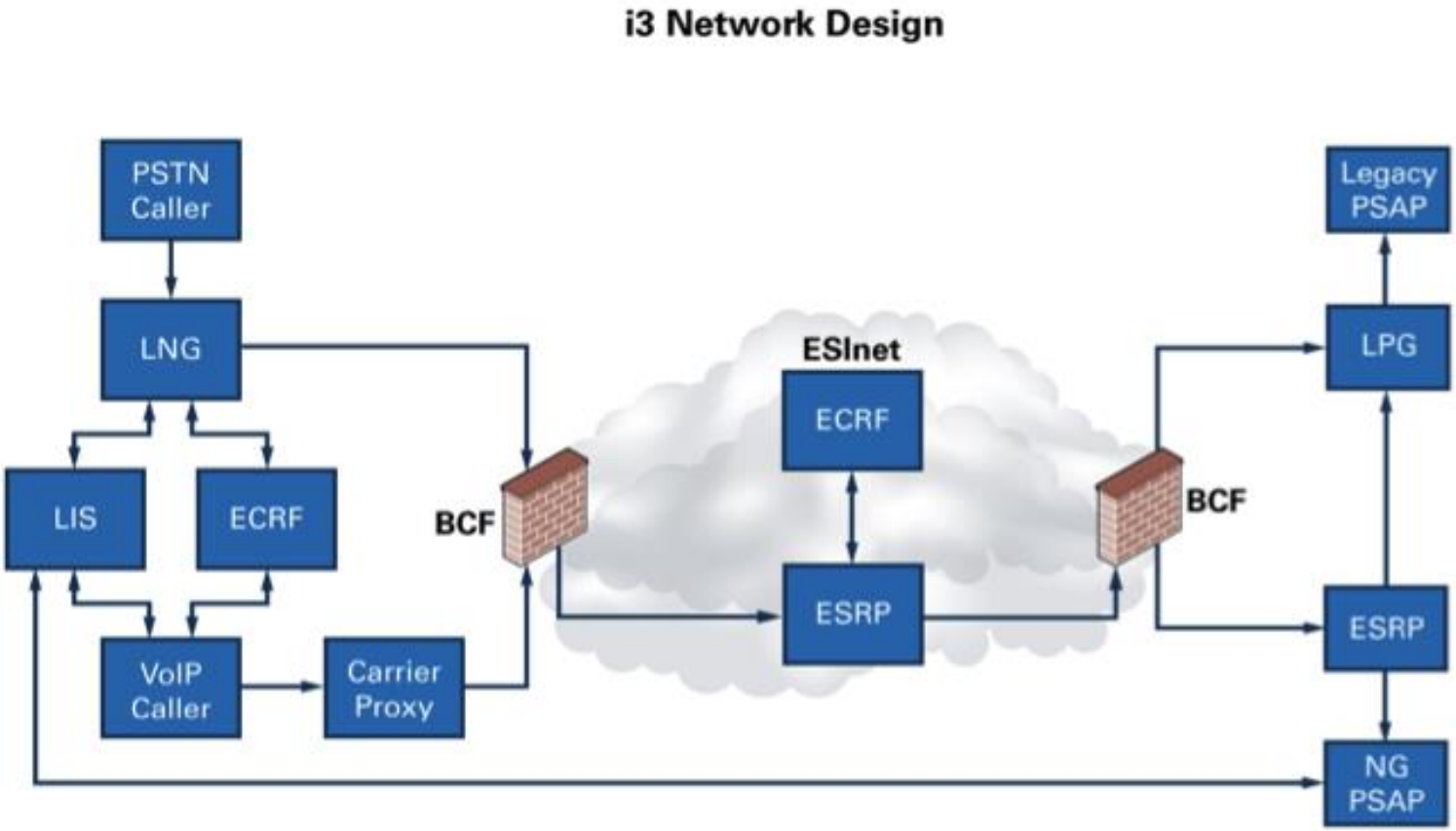
# NG9-1-1 Ecosystem



# 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 NG9-1-1 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 PSAPs

# Simplified Diagram

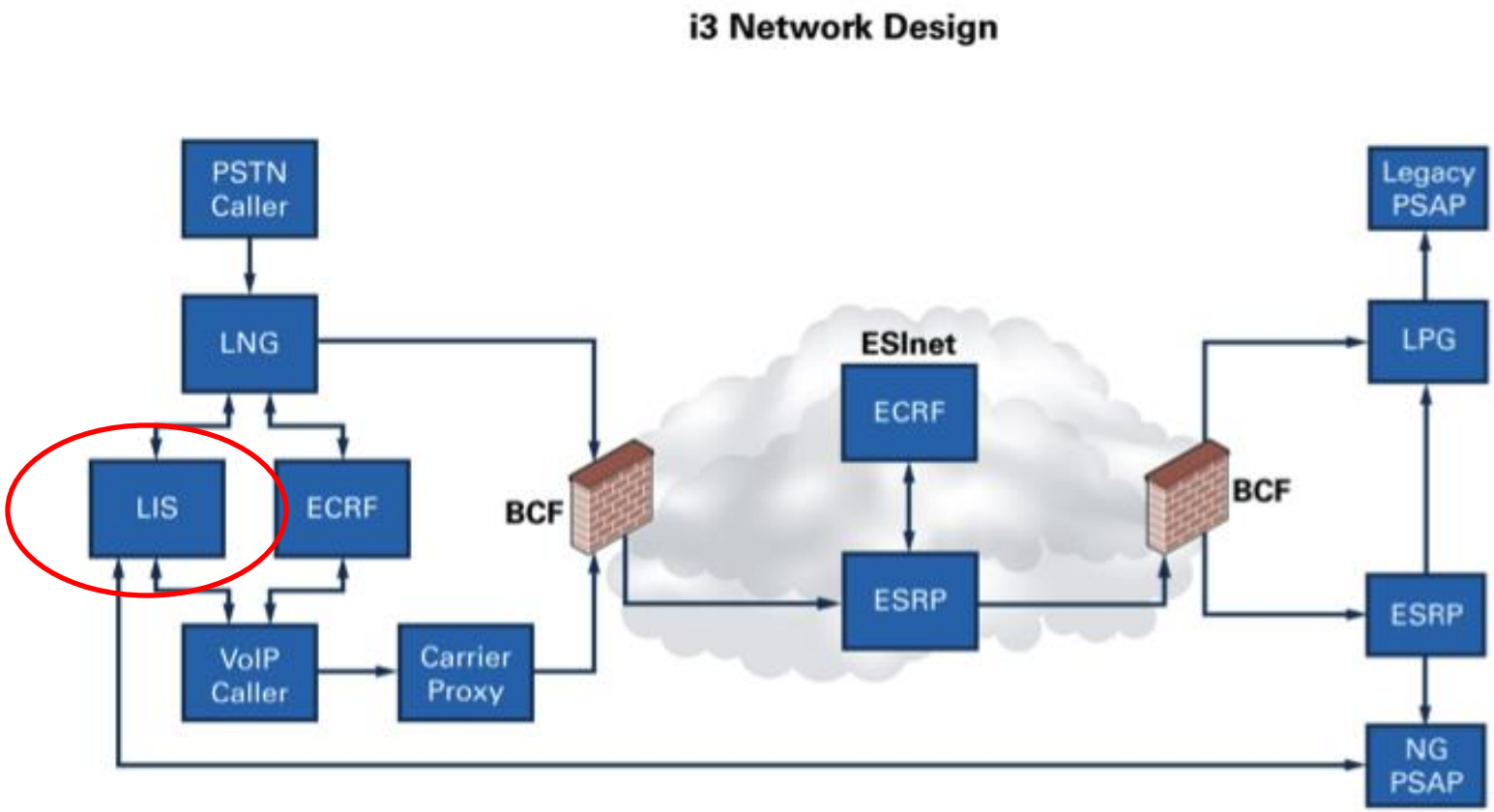



Homeland Security

OEC/ICTAP

*Office of Emergency Communications / Interoperable Communications Technical Assistance Program*

# Simplified version of i3: LIS




Homeland Security

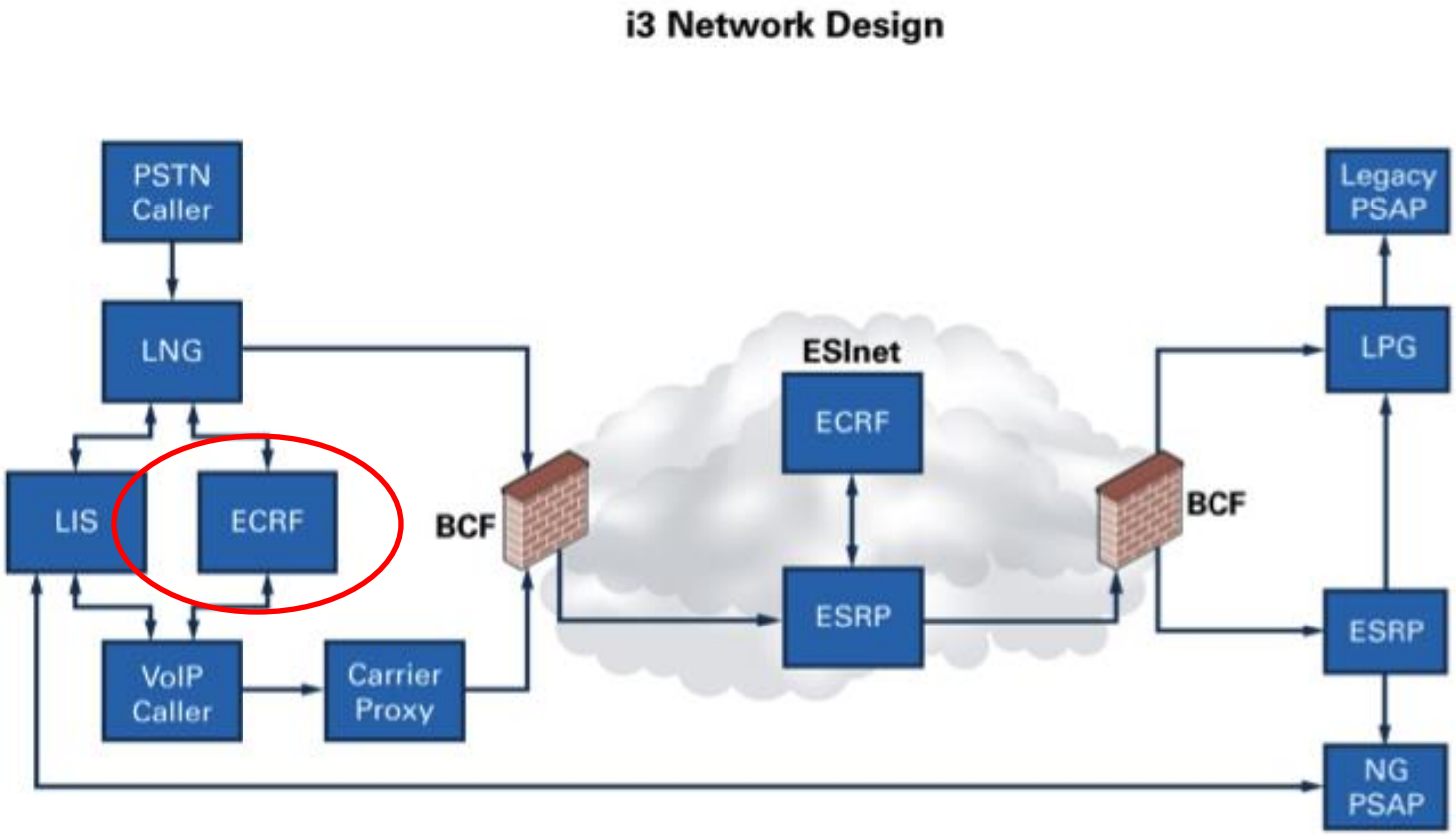
OEC/ICTAP

*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: ECRF




Homeland Security

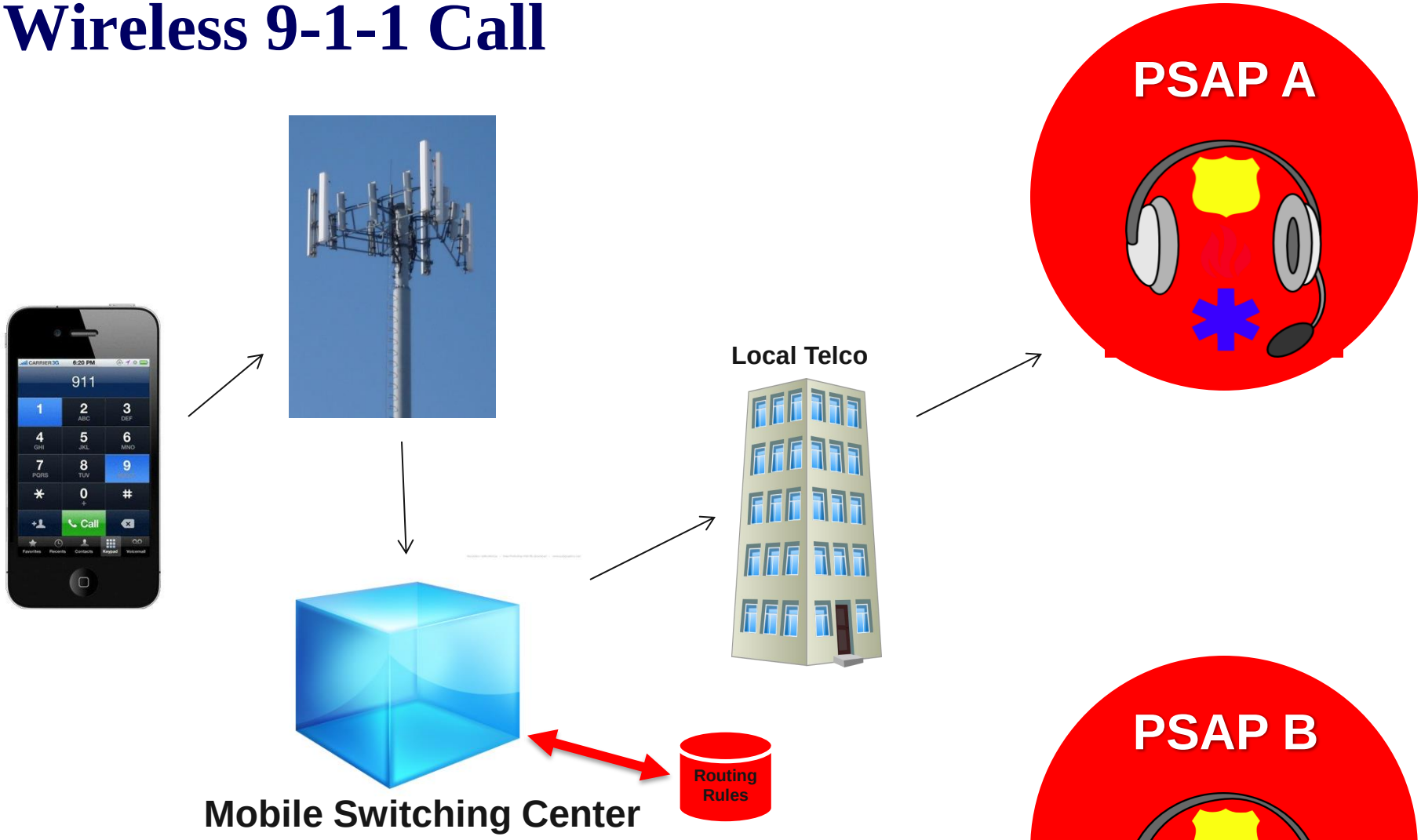
OEC/ICTAP

*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 on 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

# Wireless 9-1-1 Call

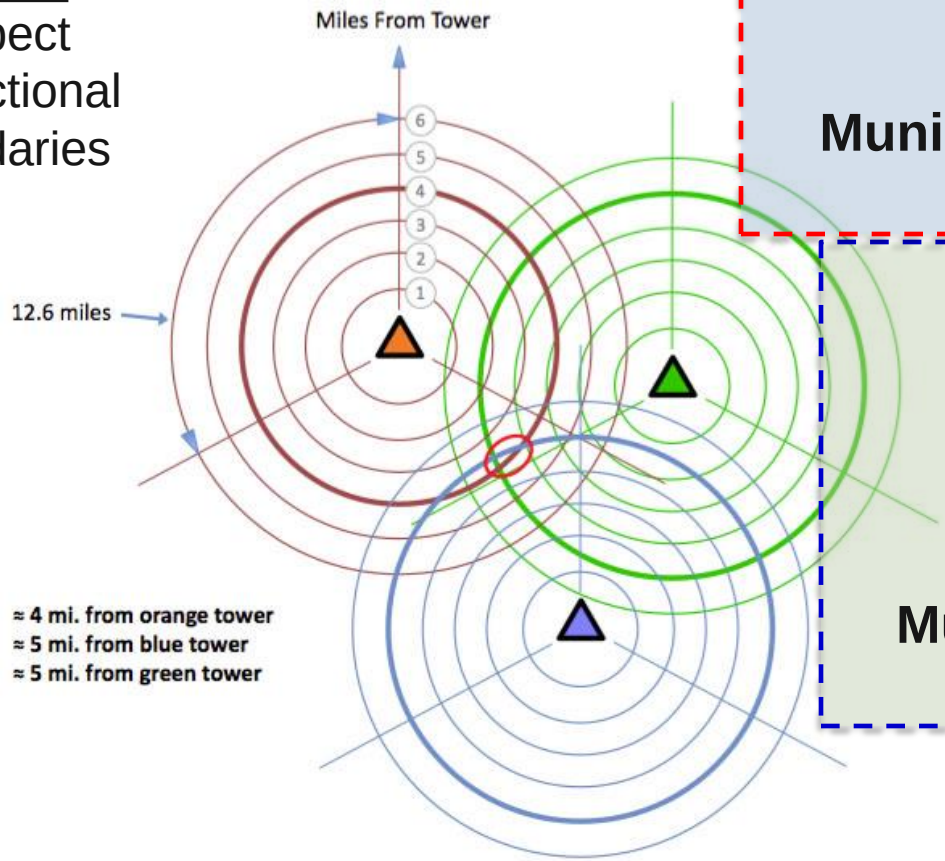



Homeland Security

OEC/ICTAP

*Office of Emergency Communications / Interoperable Communications Technical Assistance Program*

Tower Signals
**Do Not**
Respect
Jurisdictional
Boundaries



**PSAP A**

**Municipality A**

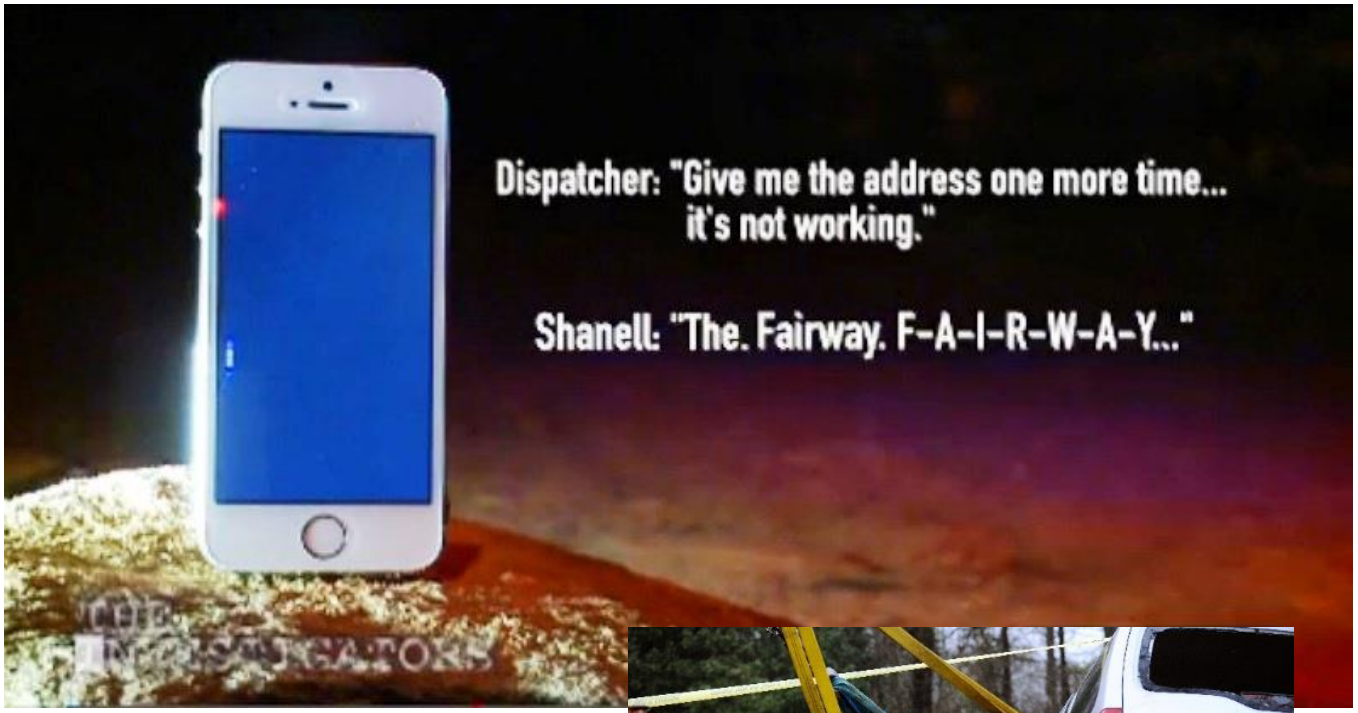
**PSAP B**

**Municipality B**

Homeland Security

OEC/ICTAP

*Office of Emergency Communications / Interoperable Communications Technical Assistance Program*

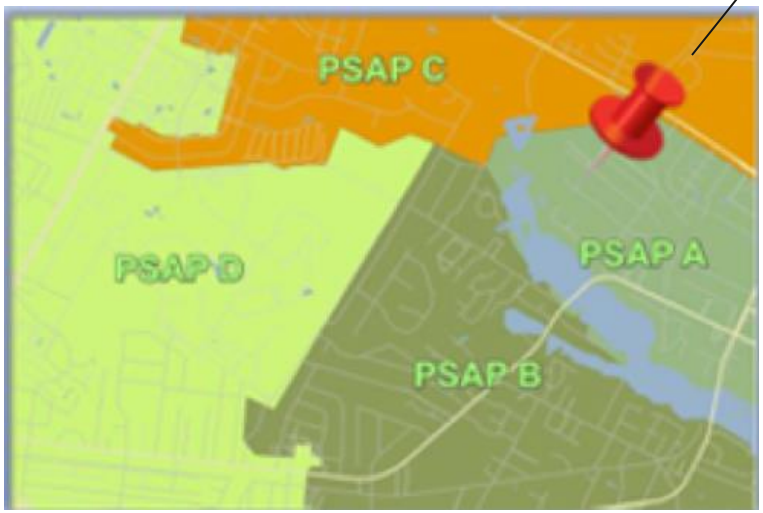


Homeland Security

**OEC/ICTAP**

*Office of Emergency Communications / Interoperable Communications Technical Assistance Program*

# Geospatial Routing



**PSAP A**

Homeland Security

**OEC/ICTAP**

*Office of Emergency Communications / Interoperable Communications Technical Assistance Program*

# Geospatial Routing

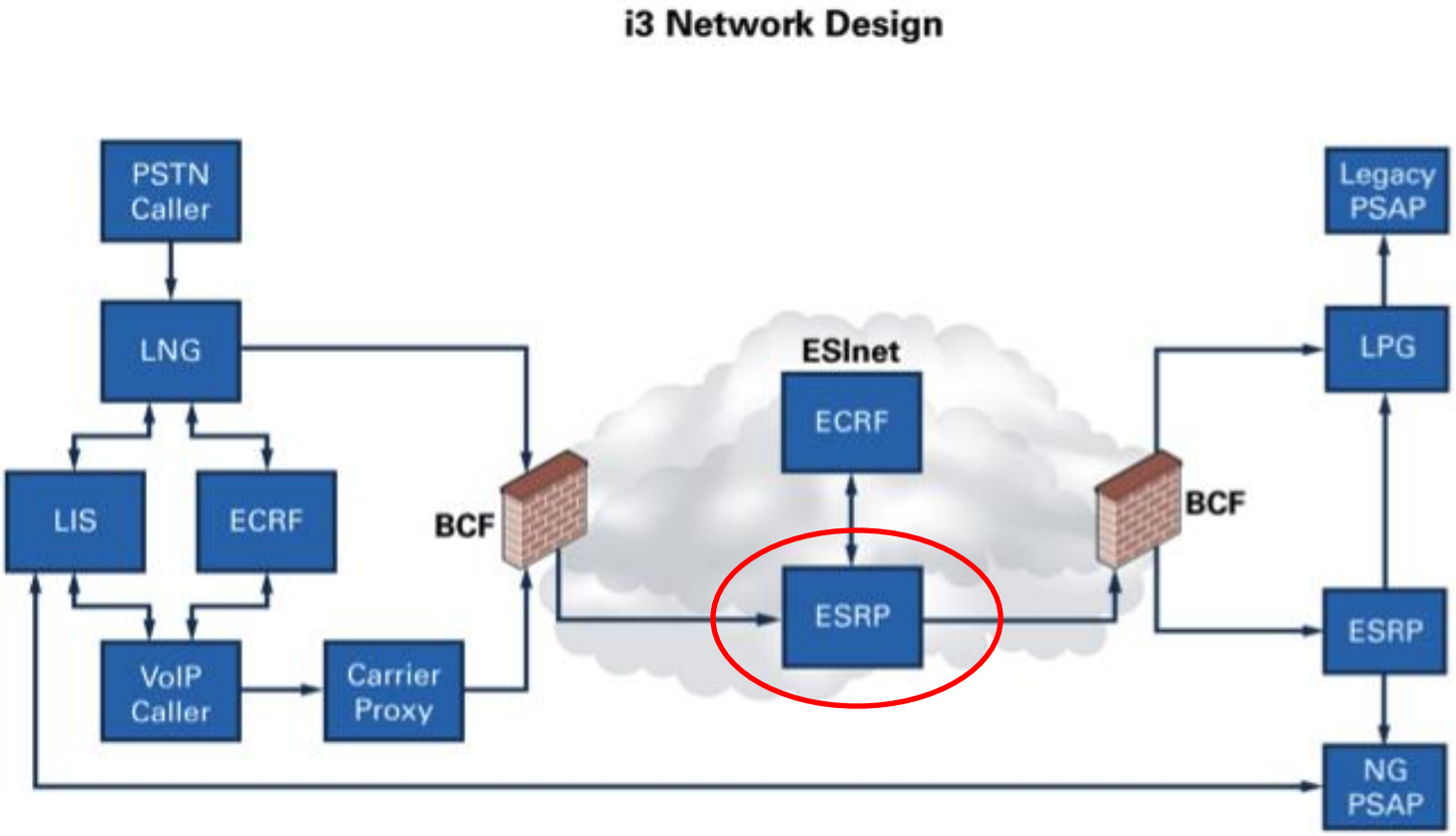
Homeland Security

OEC/ICTAP

*Office of Emergency Communications / Interoperable Communications Technical Assistance Program*

GeoFence

# Simplified version of i3: ESRP




Homeland Security

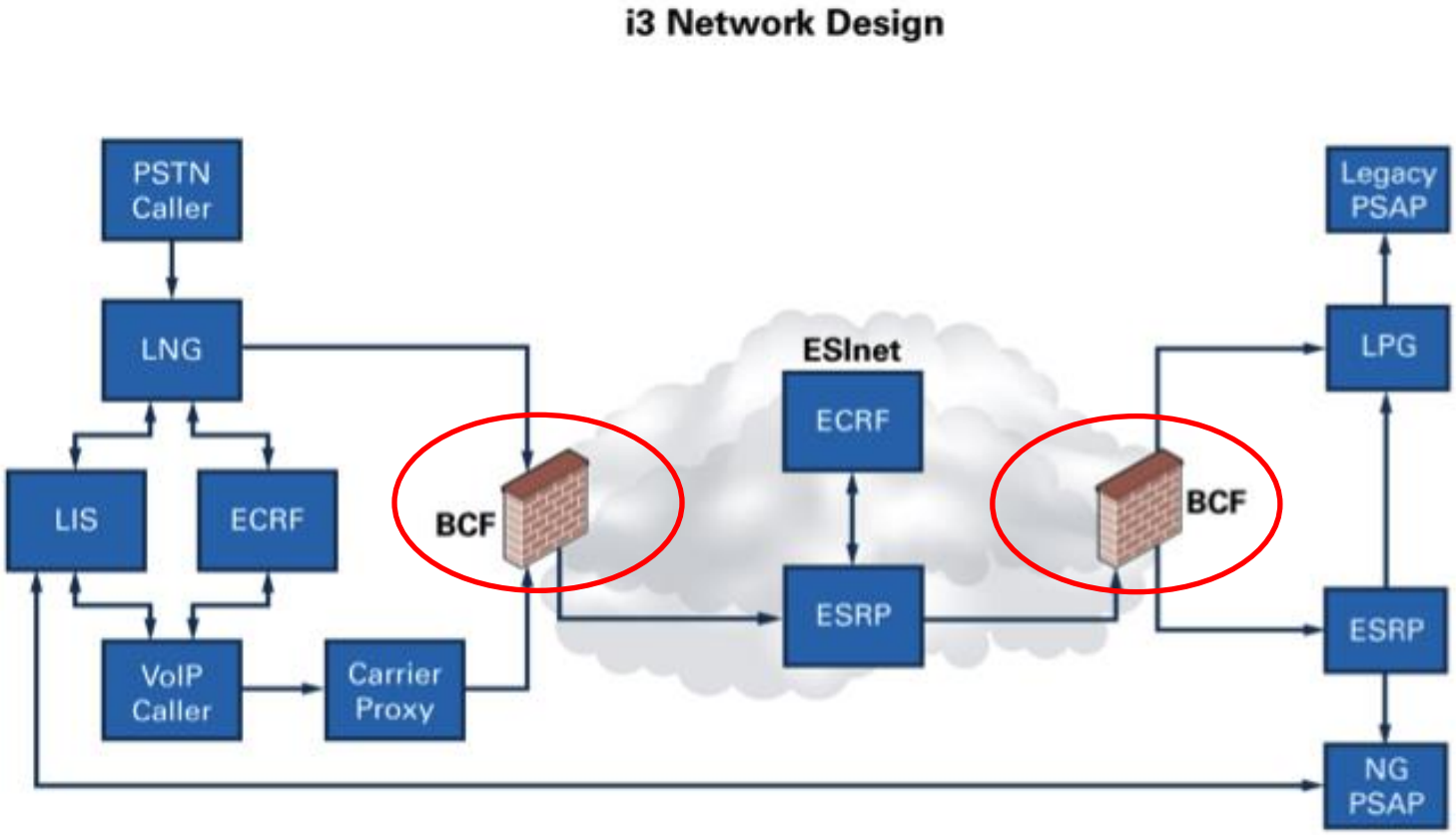
OEC/ICTAP

*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.

# Simplified version of i3: BCF




Homeland Security

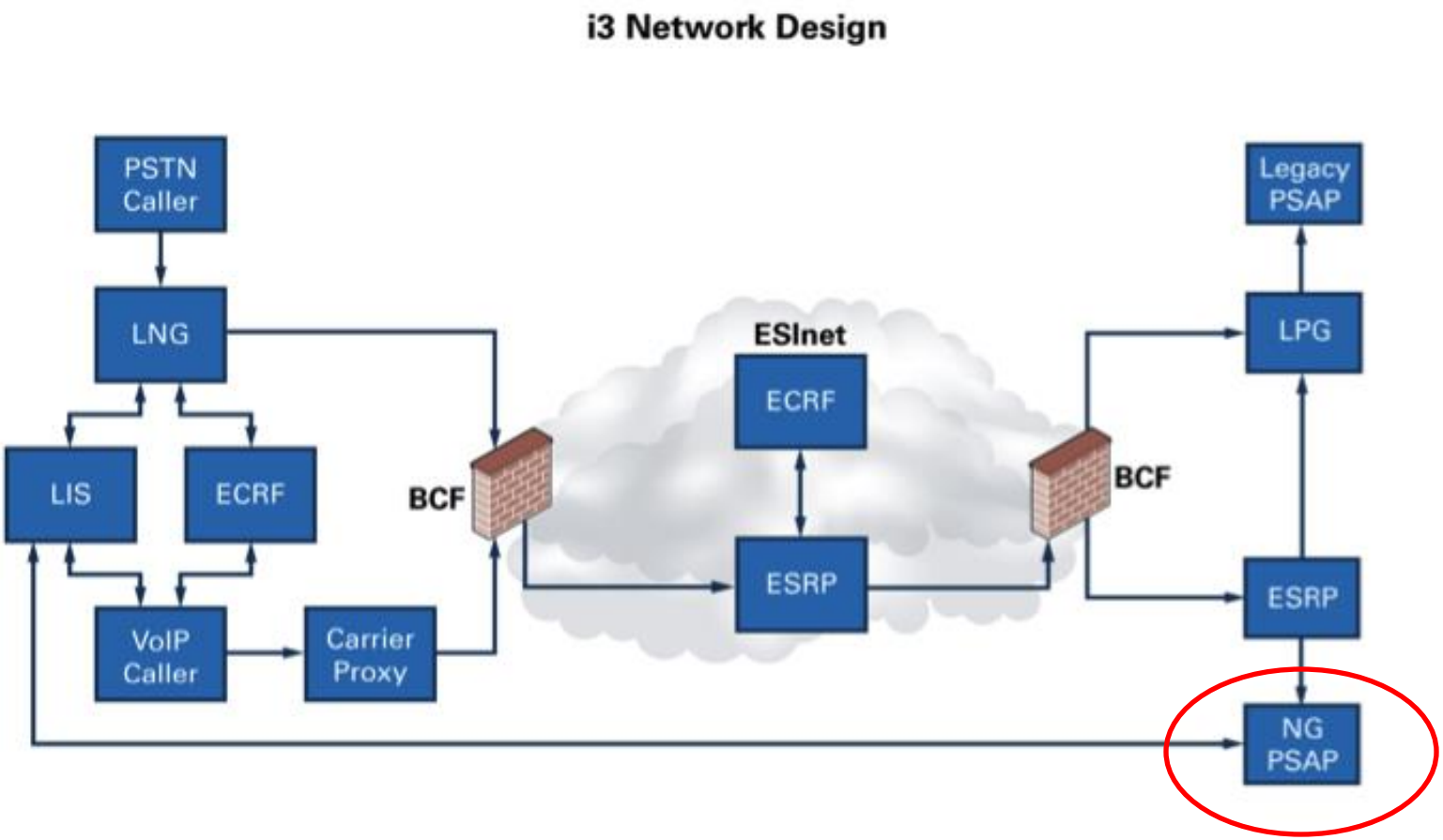
OEC/ICTAP

*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)

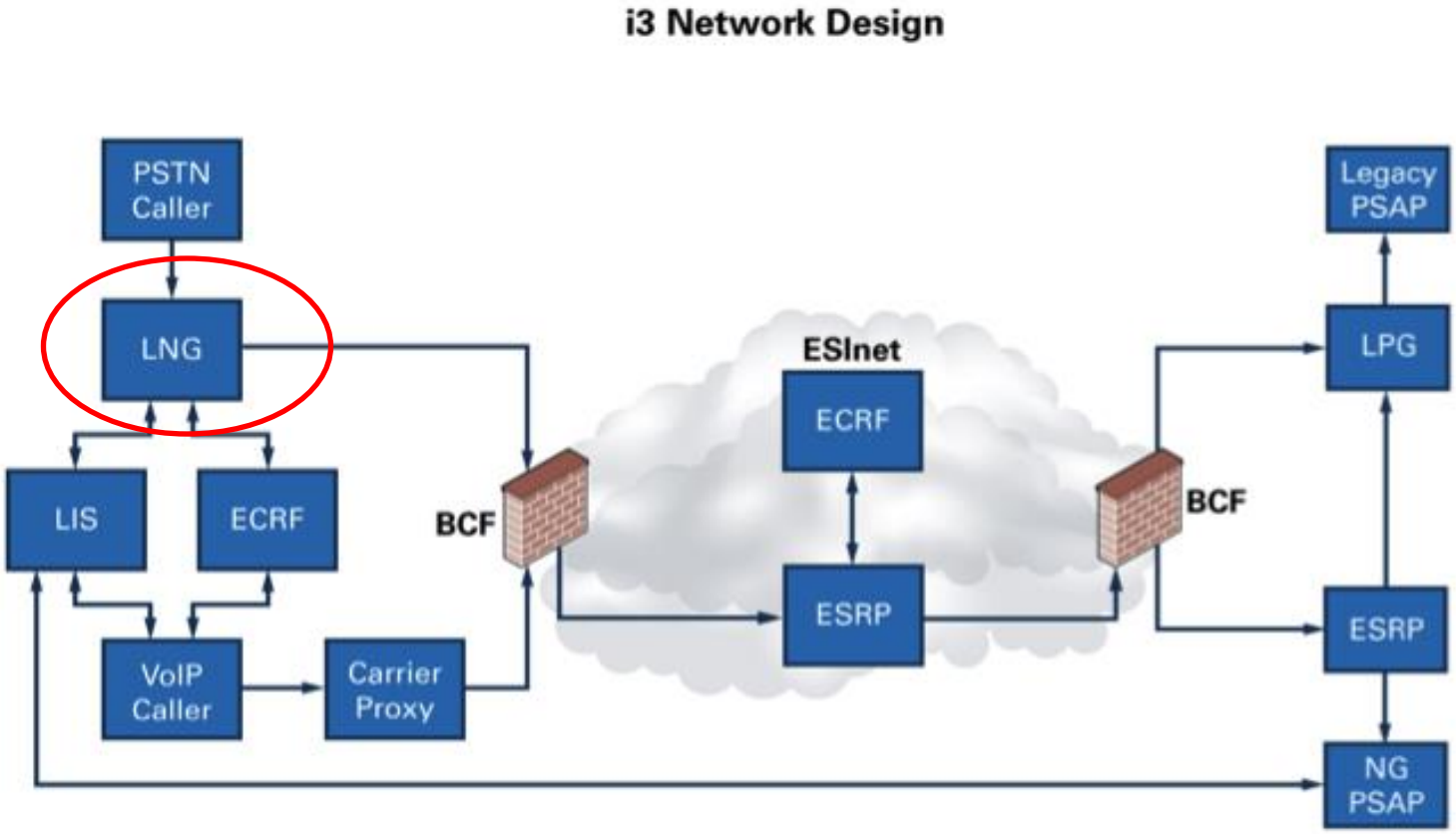
# Simplified version of i3



# 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

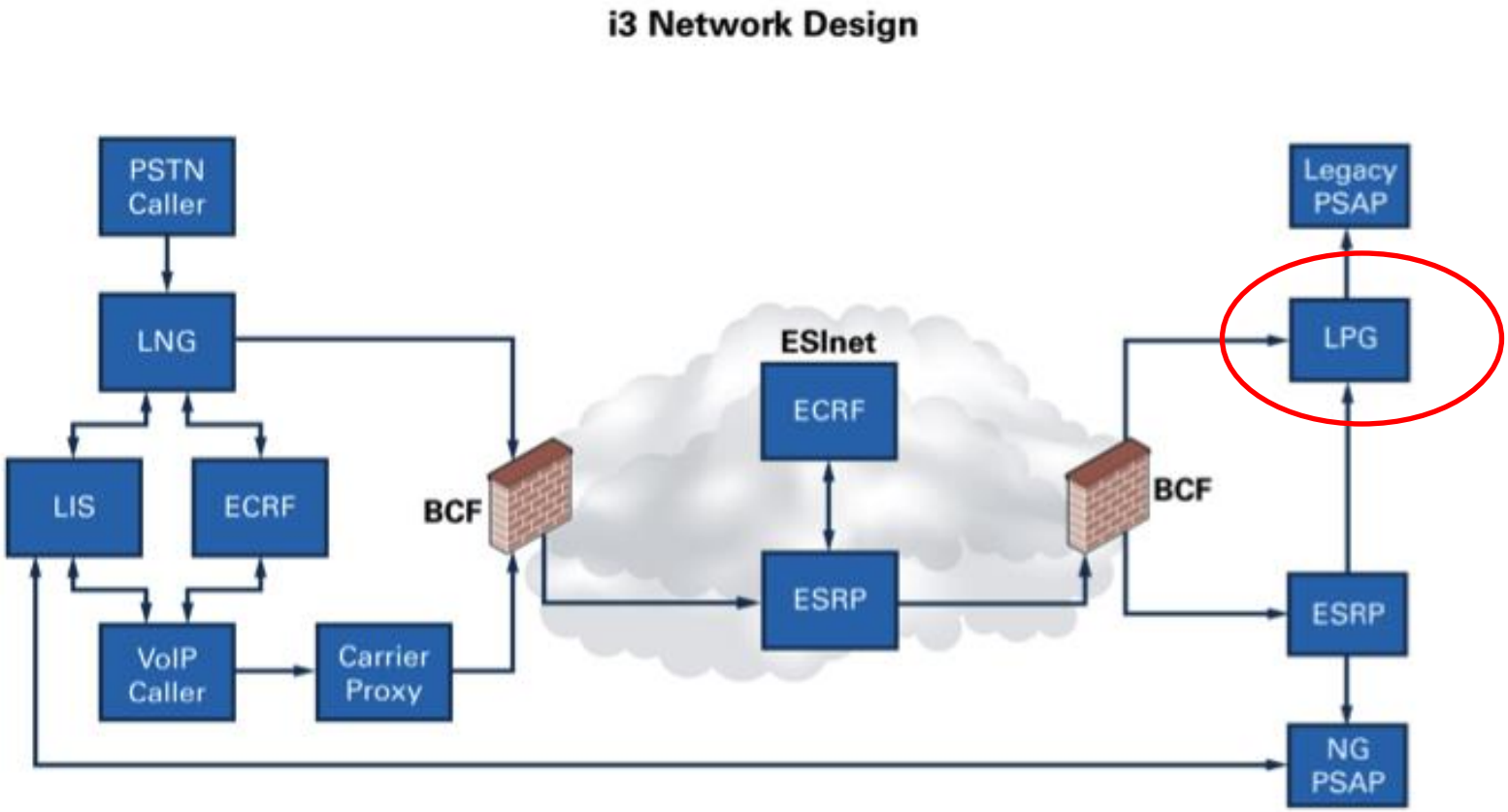
# Simplified version of i3



# 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

# 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’; 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

# 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, etc.)
- 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/her 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

# 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 NG9-1-1
  - Generally can be used to build NG9-1-1 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
  - Delivers all the information about the call

# GIS & NG 9-1-1

Homeland Security

# GIS in NG9-1-1

- Fully integrated into NG9-1-1, 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 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 NG9-1-1

- 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 NG9-1-1

- 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.

# GIS data used for call routing

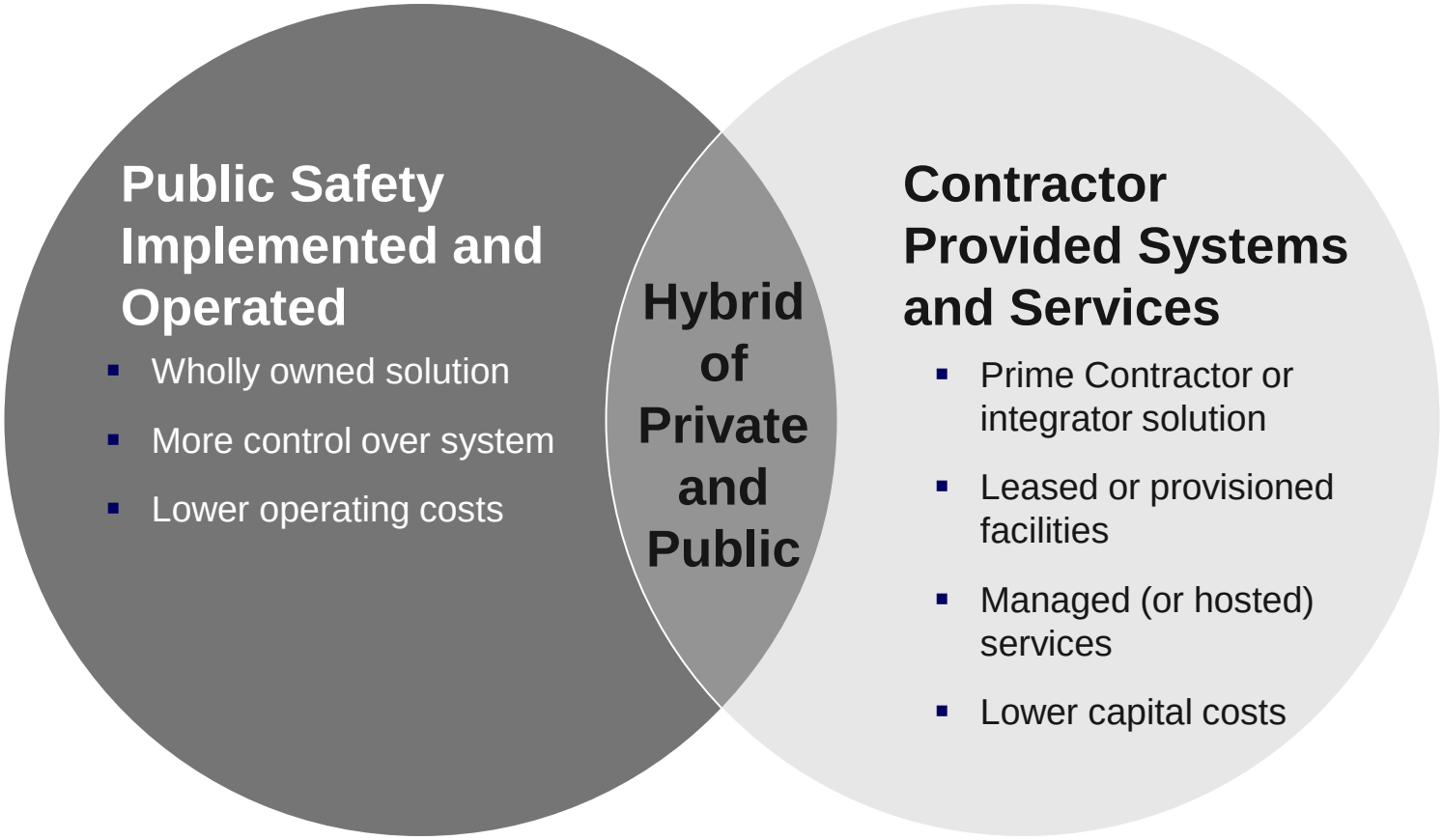
- Accuracy of data will determine correct routing of call
- GIS road centerlines, address points and jurisdictional boundaries all become focus of emergency routing databases
- What can you be doing to prepare GIS data?
  - Synchronize GIS with MSAG and ALI NENA 71-501, Version 1.1, September 8, 2009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

# Transition Planning

Homeland Security

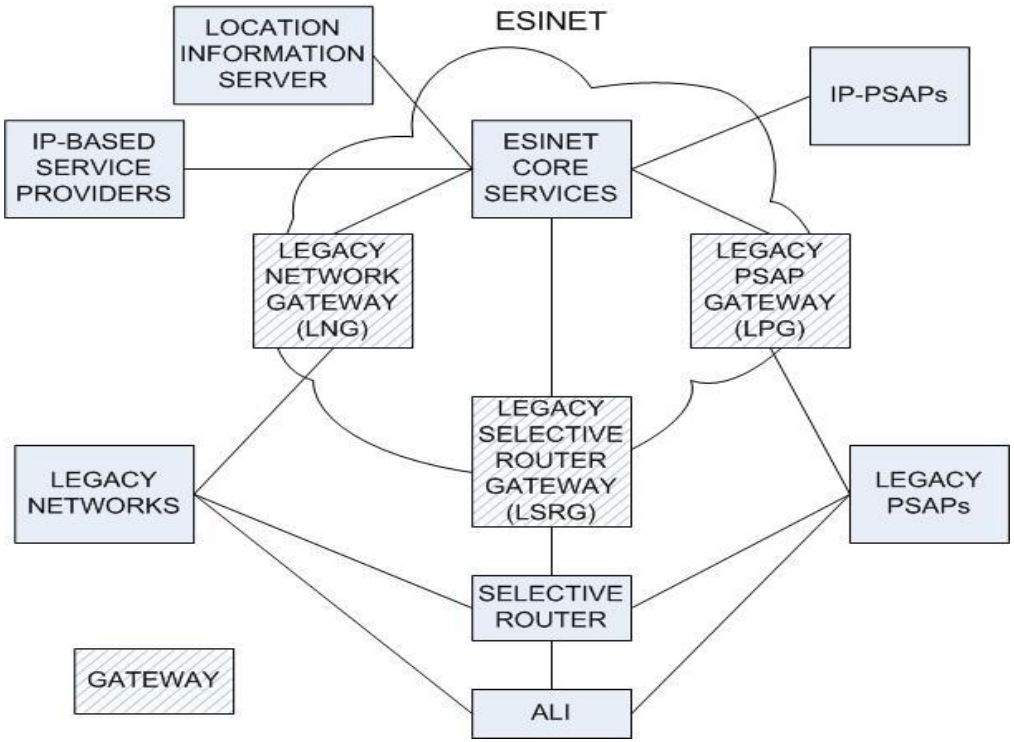
# Transition Planning

# 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 NG9-1-1 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



# NG9-1-1 Landscape Cybersecurity

# Targeting of PSAPs

- PSAP systems, like NG911, 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

# NG911's Need for Cybersecurity

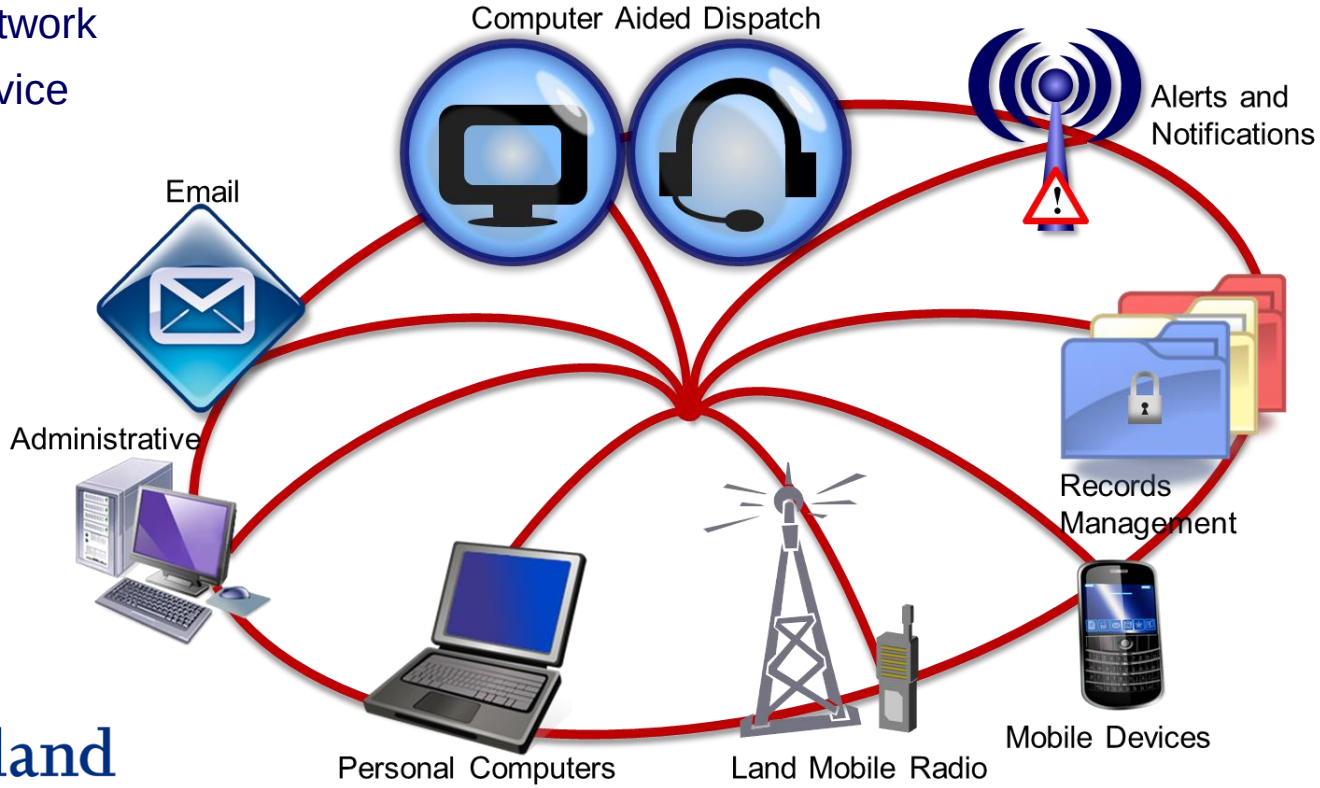
- NG9-1-1 systems rely on IP-based technologies to enable diverse multi-media, location-based services, and routing benefits
- Reliance on IP exposes NG9-1-1 PSAP systems to a new, online threat environment, creating a heightened vulnerability to attacks through IP networks
- Communication through NG9-1-1 may hide malicious threats (e.g. viruses can be embedded in texts, images, video and other files)
- NG9-1-1 systems connect with other critical systems or devices
  - Infecting one NG9-1-1 system may impact other integrated systems (i.e., records management systems)
- Threat awareness and monitoring can enable NG9-1-1 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 NG9-1-1 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<br>• Report all attacks to the FBI at www.ic3.gov<br>• Collect time, date, originating phone number, traffic characteristics of TDoS attack<br>• 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<br>• 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"<br>• Use unique passwords for different systems and sites<br>• Change passwords frequently<br>• 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

OEC/ICTAP

*Office of Emergency Communications / Interoperable Communications Technical Assistance Program*

# 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
  - **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

- 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
- 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*** if 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

# 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 NG9-1-1 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

# Questions