CSR C

Communications Security, Reliability and Interoperability Council

September 2018 WORKING GROUP 1

Transition Path to NG9-1-1

Final Report - Small Carrier NG9-1-1 Transition Considerations

Table of Contents

1 Results in Brief 4

1.1 Executive Summary 4

2 Introduction 6

2.1 CSRIC Structure 7

2.2 Working Group 1 and Task Team Members 7

3 Objective, Scope, and Methodology 10

3.1 Objective 10

3.2 Scope 11

3.2.1 Wireless Carriers (Commercial Mobile Radio Services or CMRS) 11

3.2.2 Local Exchange Companies 12

3.2.3 Cable Operators 13

3.2.4 Internet/Data Service Providers 13

3.3 Methodology 13

4 Background 14

4.1 Historical Regulatory Environment and Interconnection 15

5 Analysis, Findings and Recommendations 16

5.1 Analysis 16

5.1.1 Interconnection 16

5.1.1.1 Legacy Environment 16

5.1.1.1.1 Legacy Wireline E9-1-1 Interconnection 17

5.1.1.1.2 Legacy Small CMRS Carrier E9-1-1 Interconnection 18

5.1.1.1.3 Interim VoIP E9-1-1 Interconnection 19

5.1.1.1.4 Legacy Small Cable Operators 21

5.1.1.2 Originating Service Provider IP Interconnection for NG9-1-1 21

5.1.1.2.1 IP Interconnection to an Next Generation (NG) Emergency Services Network 22

5.1.1.2.1.1 Considerations for Interconnection 23

5.1.1.2.2 Transitional Interconnection to an NG Emergency Services Network 23

5.1.1.2.2.1 Small Carrier Hosts the LNG 26

5.1.1.2.2.2 NG Emergency Services Network Provider Hosts the LNG 26

5.1.1.2.2.3 Hosting the LNG 26

5.1.2 Call and Data Related Matters 26

5.1.2.1 LIS and LVF Validation Provisioning 27

5.1.2.2 Originating Service Provider Issues and Concerns 28

5.1.3 Security 28

5.1.3.1 NG 9-1-1 Cybersecurity Considerations 28

5.1.3.2 Recommended Practices 29

5.1.3.2.1 Cybsecurity Workforce Development 29

5.1.3.2.2 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework 30

5.1.3.2.3 NIST Cybersecurity Framework (NCF) 30

5.1.3.2.4 DHS NG9-1-1 Resources 33

5.1.4 Potential State and/or Federal NG9-1-1 Regulatory Considerations 34

5.1.5 Funding 35

5.1.6 Other Issues and Factors 38

5.1.6.1 Transition Timelines 38

5.1.6.2 Devices 39

5.1.6.3 Roaming Implications 39

5.1.6.4 Capacity Issues during Major Emergencies 40

5.1.6.5 Staff Preparation 40

5.2 Small Carrier Readiness Checklist 40

5.2.1 Stages of Readiness 41

5.2.2 Essential Elements of Readiness 42

5.2.3 Small Carrier Checklist 44

6 Conclusions 54

7 Appendix – Definitions 55

# Results in Brief

## Executive Summary

The CSRIC VI Council has been charged with defining the long term network requirements for transmitting emergency services information to emergency services organizations and personnel that is beyond communications between PSAPs, and between the public and PSAPs. Working Group 1 was charged to specifically look at service provider support for public safety transition to NG9-1-1. In that charge, the Commission directed CSRIC to recommend measures to improve both legacy 9-1-1 and NG9‑1‑1 systems, to include recommending ways in which the FCC may further the NG9-1-1 transition and enhance the reliability and effectiveness of NG9‑1‑1 through routing redundancy and maintenance and mitigate against the threat of outages to both legacy 9-1-1 and NG9-1-1 systems.

This Report evaluates the issues faced by small carriers as they update their networks to support NG9-1-1 and advises the FCC on small carrier concerns related to NG9‑1‑1 implementation, including recommendations on how the FCC can assist such originating service providers. This includes advice on what small carriers should do to be prepared to deliver their 9-1-1 traffic in an NG9-1-1 compatible manner; what economic challenges, if any, may impede small carriers in implementation of NG9-1-1; and what barriers to implementation, if any, the FCC should address.

The Working Group considered four types of small carriers providing originating communication services, including wireless carriers, local exchange companies providing wired service, television cable operators, and Internet/Data Service Providers. The report is organized around three major sections, dealing with the scope and nature of the report, analysis, findings and recommendations, and a small carrier readiness checklist structured around service provider support for migration to NG9-1-1.

The “Analysis, Findings and Recommendation” section builds on a review of today’s legacy environment, and addresses service provider interconnection with both transitionary and “end-state” NG9-1-1 systems, call and data related matters, security, and regulatory/policy factors. The Small Carrier checklist will assist small carriers into identifying attributes to be considered during the transition to support NG9-1-1.

The small carrier checklist is structured around three stages of small carrier “readiness” to support NG9-1-1, moving from today’s legacy envirorment, through transitionary deployments, to end-state NG9-1-1 public safety systems. Essential “elements” of readiness are identified, ranging from public safety governance and regulatory matters, to routing and location matters, geographic information system (GIS) needs, network considerations, security and operational planning requirements.

The highlights of the recommendations of this Report are:

* Transition Timeline

The small carrier transition timelines will vary by carrier depending on the resources they have available to focus on the transition. It is important that small carriers work with their state or regional 9-1-1 Authority to coordinate their transition timelines and expectations.

* Regulatory Environment

Historically, state and federal statutes or regulations regarding time division multiplex (TDM) network interconnection to a legacy 9-1-1 selective router in a particular Local Access and Transport Area (LATA by small carriers has often been based on the process for interconnecting with the largest ILEC in an area. As traffic exchange evolves into full IP environment, regulatory and technical expectations and responsibilities may change.

* Funding
* 9-1-1 Authorities are encouraged to understand historical cost recovery models for rural carriers and remain flexible to accommodate any economic challenges caused by the migration to NG911.
* The Commission is encouraged to review and consider updating the King County 9-1-1 demarcation ruling of 2001 to account for the transition from legacy circuit-switched networks to an all IP.[[1]](#footnote-1)
* Training/Preparedness

Included are suggestions for small carriers to prepare their staff for the NG9-1-1 transition.

* NG9-1-1 Awareness

Carriers should stay abreast of the NG9-1-1 transition to better understand the ecosystem, timelines, and implications for their companies. The Commission is encouraged to assist in industry awareness of the CSRIC recommendations.

* Implementation Schedules

Carriers should establish contact with NG9-1-1 Authorities within their service areas and gather information such as implementation schedules and functionality expectations.

* SIP Training

Carriers should consider SIP training and best practices to enable their staff to provision reliable and secure SIP trunks.

* Interconnection Options

Small carriers need to evaluate the interconnection options to the NG9-1-1 ESInet based upon negotiations with the NG9-1-1 System Service Provider (SSP). They may interconnect with native IP or via gateways based upon their own network transition plans.

* Delivering Caller Location to the NG9-1-1 ESInet

In general, the concept of NG9-1-1 is that the originating network provides the location of the caller to the ESInet for routing purposes, whether it is a fixed or mobile location. The small carriers need to work with the NG9-1-1 SSP to identify options for data management.

* Security/Cybersecurity

Carriers should prepare their staff for Cybersecurity issues related to NG9-1-1 as addressed in this Report. It is neither reasonable, nor expected, that each small carrier nationwide would be able to implement every core cybersecurity service, hire cybersecurity experts, and/or provide their own in-house version of those suggested core services. Instead, cybersecurity core services, training and capabilities will likely be a combination of the most economic, technologically sound and operationally effective technologies available. It is the intent of CSRIC to provide options and information so that small carriers can make intelligent choices, from the available options, based on their local needs and capabilities.

* Small Carrier Checklist

See section 5.2

# Introduction

The public’s access to emergency services through 9-1-1 involves many stakeholders, ranging from originating communication service providers, vendors offering supporting services, products and tools, to a variety of interconnected public safety entities responsible for the public safety systems processing calls for help, and ultimately the first responders that make up the actual response involved. The effectiveness of this paradigm depends a great deal upon how well these stakeholders and their services work together. Historically it has worked well and 9‑1-1 has both protected property and saved countless lives.

With that historical foundation, the public safety community today is involved in a migration to the “next generation” of 9-1-1 services. As the NG911 Now Coalition observes,

*NG911 is a nationwide, standards-based, all-IP emergency communications infrastructure enabling voice and multimedia communications between a 9-1-1 caller and a 911 center, and on to responders in the field.*

*Citizens in need of emergency assistance will be able to transmit photos, videos and other existing and future forms of broadband data and applications, in addition to voice, to 911 professionals. This could include streaming video from an emergency incident, photos of accident damage or a fleeing suspect, or medical information, all of which would greatly aid 911 professionals in assisting the caller or communicating with field responders and incident commanders.*

*Moreover, when a highly reliable, secure, standards-based NG911 system is deployed nationwide, 911 centers (known as “Public Safety Answering Points” or PSAPs) will have enhanced tools at their disposal for more effective and efficient response, and increased ability to interoperate with other PSAPs or transfer all functionality in the event of a major disaster.[[2]](#footnote-2)*

The faces to 9-1-1 are the communication services the public utilizes to place a 9-1-1 call. The providers of those services play a key role in emergency response. It is important that they are ready to support public safety’s migration to the next generation of 9-1-1 (NG9-1-1). Smaller originating service providers (OSPs) may be more challenged to provide that support due to service limitations and resources. In response to the FCC’s request, this report takes a look at specifically what small carriers need to be prepared to do to support NG9-1-1, both in transition, and, in full end-state environments.

## CSRIC Structure

|  |  |  |
| --- | --- | --- |
| **Communications Security, Reliability and Interoperability Council VI** | | |
| **Working Group 1: Transition Path to NG9-1-1**  ***Chair***: Mary Boyd, West Safety Services  ***FCC Liaisons***: David Furth and John Healy | **Working Group 2: Comprehensive Re-imagining of Emergency Alerting**  ***Chair:*** Farrokh Khatibi, Qualcomm  ***FCC Liaisons***: Steven Carpenter and Austin Randazzo | **Working Group 3: Network Reliability and Security Risk Reduction**  ***Chair*:** Travis Russell, Oracle  ***FCC Liaisons*:** Suzon Cameron |

Table 1 – CSRIC VI Structure

## Working Group 1 and Task Team Members

Working Group 1 consists of the members listed below.

|  |  |  |
| --- | --- | --- |
| **Name** | **Company** | **Task Group** |
| Mary Boyd, ENP  Vice President, Regulatory, Policy & Government Affairs\* | West Safety Services | Chair, WG 1 |
| Tom Breen, ENP  Member of Technical Staff; Safety & Security Technologies | Comtech Telecommunications Corp. | Task1 |
| Don Brittingham,  Vice President, Public Safety Policy\* | Verizon Communications | Task 1 |
| Budge Currier, 9-1-1 Branch Manager,  Public Safety Communications\* | California Governor’s Office of Emergency Services (CalOES) | Co-Chair, Task 1 |
| Jeroen deWitte,  VESTA Network Solutions | Motorola Solutions | Task 2 |
| Laurie Flaherty, Coordinator, National 9-1-1 Program\* | National Highway Traffic Safety Administration | Task 2 |
| Mark J. Fletcher,  Chief Architect  Worldwide Public Safety | Avaya | Task 1 |
| Matthew Gerst, Assistant Vice President,  Regulatory Affairs | CTIA | Task 1 |
| James D. Goerke, Chief Executive Officer | Texas 9-1-1 Alliance | Co-Chair, Task 2 |
| Dan Henry, Director of Government Affairs & Information Security Issues\* | National Emergency Number Association (NENA) | Task 1 & 2 |
| Karima Holmes, Director | Office of Unified Communications, Government of Washington, DC | Task 1 |
| Michael Hooker, Member of Technical Staff | T-Mobile USA, Inc. | Task 1 & 2 |
| Chris Kindelspire, Director Electronic Operations | Grundy County ETSB | Task 1 |
| William Andrew Leneweaver, Deputy State 9-1-1 Coordinator for Enterprise Systems | Washington StateE9-1-1 Coordination Office | Task 1 |
| Tim Lorello, President and Chief Executive Officer, SecuLore Solutions | Industry Council for Emergency Response Technologies (iCERT) | Task 1 |
| Walter Magnusen, Ph.D., Director, Texas A&M University Internet2 Technology Evaluation Center\* | Texas A & M University | Co-Chair, Task 1 |
| Charles P. (“Peter”) Musgrove, Lead Member of Techical Staff | AT&T Services, Inc*.* | Task 1 |
| Mike Pollock , Chief Operating Officer | Nex-Tech | Task 2 |
| Theresa Reese, Senior Engineer | Ericsson | Task 1 |
| Francisco Sanchez, Public Information Officer and Director’s Liaison\* | Harris County Office of Homeland Security & Emergency Management | Task 1 |
| Charlie Sasser, Senior Officer  Georgia Technology Authority | National Public Safety Telecommunications Council (NPSTC) | Task 1 & 2 |
| Dorothy Spears-Dean, Ph.D., Public Safety Comms Coordinator, Virginia Information Technologies Agency\* | National Association of State 9-1-1 Administrators (NASNA) | Co-Chair, Task 2, Task 1 |
| Jay English, Chief Technology Officer\* | APCO International | Task 1 |

Table 2 - List of Working Group Members

\*Indicates a member of the CSRIC Council

Working Group 1 would also recognize the valued participation and contributions of the following subject matter experts whose contributions were invaluable to the drafting and recommendations contained within the report.

|  |  |  |
| --- | --- | --- |
| Patrick Donovan, Senior Director, Regulatory Affairs | CTIA | Task 1 |
| Holly E. Wayt, RPL, ENP Communications Manager City of Westerville | APCO International  2nd Vice President | Task 1 |
| Hallie Frazee, Emergency Public Information Planner | Harris County, Office Homeland Security, Emergency Management | Task 1 |
| Roger Hixson, ENP  Technical Issues Director | National Emergency Number Association (NENA) | Task 1 & 2 |
| Richard Muscat, Director of Regulatory Affairs | Bexar Metro 9-1‑1 Network  Texas 9-1-1 Alliance | Task 2 |
| Robert Sherry, Senior Systems Engineer | West Safety Services | Task 1 & 2 |

Working Group 1 would also recognize the dedication and support provided by FCC Liasons:

|  |  |  |
| --- | --- | --- |
| David Furth, Deputy Chief  Public Safety Homeland Security Bureau | Federal Communications Commission | Task 1 & 2 |
| John Healy  Associate Division Chief in the Cybersecurity & Communications Reliability Division, Public Safety and Homeland Security Bureau | Federal Communications Commission | Task 1 & 2 |

# Objective, Scope, and Methodology

## Objective

The CSRIC VI has been charged with defining the long term network requirements for transmitting emergency services information to emergency services organizations and personnel that is beyond communications between PSAPs, and between the public and PSAPs. This includes the identification of architectures that will be able to transmit the needed information about emergency events to all persons and agencies that need it, and to aid in coordinating emergency services activities.

Specifically, CSRIC Working Group 1 was charged to look at service provider support for public safety transition to NG9-1-1. In that charge, the Commission directed CSRIC to recommend measures to improve both legacy 9-1-1 and NG9‑1‑1 systems, to include recommending ways in which the FCC may further the NG9-1-1 transition and enhance the reliability and effectiveness of NG9-1-1 through routing redundancy and maintenance and mitigate against the threat of outages to both legacy 9-1-1 and NG9-1-1 systems. The FCC also directs CSRIC to recommend actions the FCC could take to encourage the private sector to detect or deter threats to 9-1-1 before they reach the ESINet perimeter. The focus is on identifying tools that are already available or not burdensome to implement, and on developing a set of best practices for carriers and 9-1-1 service providers.

In addition, the FCC directed CSRIC to advise the FCC on small carrier issues related to NG9‑1‑1 implementation, including recommendations on how the FCC could address these challenges. This is to include advice on what small carriers should do to be ready on time to deliver their 9-1-1 traffic in an NG9-1-1 compatible manner; what economic disadvantages, if any, may impede small carriers in the implementation of NG9-1-1; and what barriers to implementation, if any, the FCC should address. CSRIC was also asked to recommend an “NG9-1-1 readiness checklist” for small carriers analogous to the one the Task Force on Optimal Public Safety Answering Point Architecture (TFOPA) developed for PSAPs. This report addresses that part of the charge, including small carrier issues and the referenced readiness checklist.

## Scope

As described above, the second task of Working Group 1 involved studying and developing recommendations for the CSRIC’s consideration on small carrier processes for managing the transition to NG9-1-1. This included advice on what small carriers should do to be ready on time to deliver their 9-1-1 traffic in an NG9-1-1-compatible manner; what economic disadvantages, if any, may impede small carriers during implementation of NG9-1-1; and what barriers to implementation, if any, the FCC should address. The FCC also directed CSRIC to recommend an NG9-1-1 readiness checklist for small carriers analogous to the one the Commission’s Task Force on Optimal PSAP Architecture (TFOPA) developed for PSAPs.[[3]](#footnote-3)

The Working Group considered four types of carriers providing originating communication services, including wireless carriers, local exchange companies providing wired service, television cable operators, and Internet/Data Service Providers. In each of those service types, the Working Group focused on small providers as described below:

### Wireless Carriers (Commercial Mobile Radio Services or CMRS)

The Commission has referred to CMRS providers that offer such service nationwide as Tier I; CMRS providers that are non-nationwide mid-sized carriers with greater than 500,000 subscribers as Tier II; and CMRS providers that are non-nationwide small CMRS carriers with no more than 500,000 subscribers as Tier III.[[4]](#footnote-4) Beyond these carriers, the Commission, in its twentieth “Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services” noted that

*. . . U.S. Cellular, currently the fifth largest service provider in the United States, is best characterized as a multi-regional service provider. It has developed wireless networks and customer service operations in portions of 23 states.47 As of December 31, 2016, U.S. Cellular provided services to its customers with approximately five million connections.48 C Spire, the sixth largest service provider nationwide, provides service in the Southeastern United States to nearly one million subscribers.[[5]](#footnote-5)*

With that in mind, the Working Group considered such Tier II carriers (along with Tier I providers) to be largely national in scale, and thus outside the scope of this report, and focused on Tier III CMRS providers.[[6]](#footnote-6)

### Local Exchange Companies

In *47 USC § 153(44)* a “rural telephone company” is defined as a local exchange carrier operating entity that (A) provides common carrier service to any local exchange carrier study area that does not include either (i) any incorporated place of 10,000 inhabitants or more, or any part thereof, based on the most recently available population statistics of the Bureau of the Census, or (ii) any territory, incorporated or unincorporated, included in an urbanized area, as defined by the Bureau of the Census; (B) provides telephone exchange service, including exchange access, to fewer than 50,000 access lines; (C) provides telephone exchange service to any local exchange carrier study area with fewer than 100,000 access lines; or (D) has less than 15 percent of its access lines in communities of more than 50,000 on February 8, 1996.[[7]](#footnote-7) The Working Group considered “rural telephone companies” providing wired service as described above to be within the scope of this report.[[8]](#footnote-8)

### Cable Operators

In *47 CFR 76.901(f)* a “small cable operator” is defined as “an operator that, directly or through an affiliate, serves in the aggregate fewer than 1 percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000.” The Working Group considered small cable operators as described above to be within the scope of this report.[[9]](#footnote-9)

### Internet/Data Service Providers

In addressing this group, there does not appear to be a firm statute or Commission precedent defining a subset of these providers that should be considered small or rural in nature. With that in mind, the Working Group looked to the recent “Small Business Exemption Order” that granted an enhanced reporting requirements waiver to smaller broadband Internet access service (BIAS) providers with 250,000 or fewer broadband subscribers.[[10]](#footnote-10) That seemed reasonable to the Working Group, and was included in the scope of this report.

## Methodology

How small carriers transition to support NG9-1-1 Emergency Services depends on many factors, including the nature of the carrier involved, the existing regulatory environment, technical differences among those small carriers, and the timing and transitional approaches employed by the serving 9-1-1 Authorities.

With that in mind, the methodology of this Report focused upon four small carrier stakeholders types providing the following services: wireline, CMRS, interconnected VoIP and cable. This Report includes a brief review of historical regulatory considerations to set a baseline for analysis. It explores existing interconnection methods in order to extrapolate those into recommendations to interconnect with NG9-1-1. Based upon the above analysis, the Working Group created check lists that the stakeholders may use when considering the transition to support NG9-1-1.

Regarding cybersecurity, this report’s methodology was based on review of cybersecurity frameworks and best practices from multiple sources including the National Istitute of Standards and Technology (NIST), the Department of Homeland Security (DHS), CSRIC, and other sources. From that, the Working Group developed a set of recommended cybersecurity practices. These recommendations identified resources and tools for the development of a small carrier cybersecurity strategy specific to the NG9-1-1 ecosystem. The Working Group has also leveraged the NICE Cybersecurity Workforce Framework to provide guidance for small carrier cybersecurity workforce development and training plans.

Recognizing that small carrier representatives in the Work Group were limited, the final working draft of this report was provided to representatives of four service provider associations serving small carriers for review prior to publishment.

# Background

As the National Emergency Number Association (NENA) observes,

*The evolution of emergency calling beyond the traditional voice 9‐1‐1 call has caused the recognition that our current E9‐1‐1 system is no longer able to support the needs of the future.   Next Generation 9‐1‐1 (NG9‐1‐1) networks replace the existing narrowband, circuit switched 9‐1‐1 networks which carry only voice and very limited data.[[11]](#footnote-11)*

NG9-1-1 is defined in many ways by a wide variety of stakeholders involved and/or interested in the migration. Working Group 1 (WG1) looked to the definition adopted by the “NG911 Now Coalition.” They defined NG9-1-1 servicesas a secure, IP-based, open-standards system comprised of hardware, software, data, and operational policies and procedures that:

* provides standardized interfaces from emergency call and message services to support emergency communications;
* processes all types of emergency calls, including voice, text, data, and multimedia information;
* acquires and integrates additional emergency call data useful to call routing and handling;
* delivers the emergency calls, messages, and data to the appropriate public safety answering point and other appropriate emergency entities based on the location of the caller;
* supports data, video, and other communications needs for coordinated incident response and management; and interoperates with services and networks used by first responders to facilitate emergency response.[[12]](#footnote-12)

Originating service providers play a key role in emergency communications. As telecommunications service providers, they are responsible for delivering emergency calls to 9‑1-1 systems in accordance with nationally adopted standards. Such standards address both how and where the call is delivered – matters of call structure and interconnection. Meeting these call delivery standards may create challenges for small service providers struggling to upgrade their own services.[[13]](#footnote-13) In accordance with the Working Group’s charge described above, this report focuses on small carrier issues impacted by NG9‑1‑1 implementation.

## Historical Regulatory Environment and Interconnection

Historical state and federal statutes or regulations regarding TDM network interconnection to a legacy 9-1-1 selective router in a particular LATA by small carriers has often matched interconnection with the largest ILEC in an area. Under the 1996 Act, the FCC has set guidance and policies on TDM interconnection, and state public utility commissions often implement interconnection accordingly.[[14]](#footnote-14) While the small carrier is usually responsible for connecting to a meet point (e.g., the 9-1-1 selective router), there have been instances where such roles and responsibilities may be reversed.[[15]](#footnote-15) Where TDM-to-TDM interconnection has been the traditional interconnection scenario, IP-based providers have had the responsibility to deploy a gateway that converts IP to TDM in order to interconnect and exchange traffic with ILECs within the LATA involved. Legacy LATA regulatory issues may not only impact network interface but also data flow.[[16]](#footnote-16) With regard to the latter, some state public utility commissions, for example, may have specific requirements that a Master Street Address Guide (MSAG) be provided to small wireline carriers at no additional cost,[[17]](#footnote-17) and that there be no additional charges to the small wireline carriers for storing Automatic Location Information (ALI) and related records in a legacy 9-1-1 database.[[18]](#footnote-18) In other states, the responsibility for costs and charging issues could be completely reversed with small carriers paying the ILEC or a third-party for extra copies of the MSAG and for storing those records in the legacy 9-1-1 databases.[[19]](#footnote-19)

# Analysis, Findings and Recommendations

## Analysis

### Interconnection

This section discusses interconnection methods between a small carrier network and an Emergency Services Network. Interconnection methods for E9-1-1 are discussed in order to contrast the existing methods of interconnection with those that will be required in NG9-1-1. Four categories of originating service providers are discussed: wireline, CMRS wireless, interconnected VoIP and cable operators.

#### Legacy Environment

E9-1-1 was originally introduced to support wireline emergency calls. The concept included validating the customer’s address and placing the TN/address association in a database which could be queried by the PSAP when it received the emergency call. As wireless technologies were introduced the concept of wireline E9-1-1 was extended to support wireless calls. Since callers’ locations were dynamic, the wireline E9-1-1 concept was expanded to query the wireless databases in the CMRS network to obtain the caller’s location. As interconnected VoIP was introduced, the wireless E9-1-1 concept was extended to support VoIP callers. That is, when the PSAP received the emergency call, a database within the VoIP Service Provider (VSP) network was queried to obtain the caller’s location.

Selective Routers (SRs), also known as E9-1-1 Tandems, are a critical element of legacy Emergency Services Networks that support E9-1-1 Service. SRs are specially-equipped central offices that provide the switching of 9-1-1 calls. Selective routing is the process by which 9-1-1 calls are routed to the appropriate PSAP (or other designated destination) based on the caller’s location. For emergency calls that originate in legacy wireline networks, the caller’s location is represented by their 10-digit telephone number or Automatic Number Identification (ANI). For emergency calls that originate in legacy CMRS networks, selective routing is done based on a 10-digit location key that uniquely represents the call and allows the call to be routed to the appropriate PSAP. For emergency calls that originate in interconnected VoIP networks, selective routing is done based on a 10-digit location key that uniquely represents the call and allows the call to be routed to the appropriate PSAP.

The Database Management System (DBMS) is responsible for validating wireline callers’ addresses to assure that the location received by the PSAP is valid and can be used to dispatch First Responders. Inherent within the DBMS is a MSAG. The MSAG contains street address ranges that can be used to determine that a location is valid. Typically, an extract of new service orders is sent to the DBMS containing callers’ addresses and telephone numbers. All of the addresses in this extract are validated against the MSAG and any inconsistencies are managed by the E9-1-1 SSP. Once an address is validated, it is assigned an Emergency Service Number (ESN) which is used for routing. Once an address has been validated and assigned an ESN the TN/ESN association is pushed to the Selective Router Database (ERDB) and the telephone/address association is pushed to the Automatic Location Identification (ALI) database. For wireless calls since locations are geodetic, and potentially dynamic, no validation occurs. For interconnected VoIP calls, the validation takes place in the VSP network.

The ALI database is a repository for the telephone/address relationship as well as a pseudo message switch that can “steer” location requests to external servers (e.g., Mobile Positioning Center (MPC), Global Mobile LocationCenter (GMLC), and VoIP Positioning Center (VPC)) that contain the caller’s location. When the PSAP receives a call the PSAP CPE queries the ALI database. If the location is contained within the ALI database (i.e., TN/address association) the ALI database will return the address to the PSAP. If the call was placed via Interim VoIP or wireless, the ALI database will query the external server and return the location provided by that server.

##### Legacy Wireline E9-1-1 Interconnection

The figure below illustrates the interconnection between a small wireline carrier (e.g., Competitive Local Exchange Carrier [CLEC] or independent telephone company) network and the legacy Emergency Services Network. The delivery of the wireline 9-1-1 caller’s telephone number allows PSAPs to access the location information associated with the telephone number by querying the ALI database. In the case of wireline emergency callers, the ALI database contains static telephone number-to-street address mappings.

Typically, the small wireline carrier will have a Service Order Interface (SOI) to the DBMS of the E9-1-1 SSP. The small wireline carrier will send TN/address associations of its customers to the DBMS which will validate them, assign an ESN and push the TN/ESN associations to the Selective Router Database (SRDB) and the TN/address associations to the ALI database. The management of this process must be agreed upon between the small wireline carrier and the E9-1-1 SSP.

For call routing, the small wireline carrier will have either SS7 or MF interconnection to the SR of the E9-1-1 SSP. The interconnection points must be agreed upon between the small wireline carrier and the E9-1-1 SSP. When its customer makes a 9-1-1 call, the small wireline carrier switch will forward the call to the SR with the TN. The legacy Emergency Services Network will then use this information to route the call to the appropriate PSAP and the PSAP will use this information to query for the ALI information.



##### Legacy Small CMRS Carrier E9-1-1 Interconnection

Enhanced wireless emergency services (i.e., wireless E9-1-1) requires small or regional CMRS carriers to provide an approximate location of the wireless 9-1-1 callers to PSAPs. For the initial stage, Phase I, the FCC required CMRS carriers to upgrade their networks to support delivery of a callback number and an identifier of the cell site or base station location where the 9-1-1 call originated to the PSAP. Phase II requires delivery of E9-1-1 services that includes the latitude and longitude of the 9-1-1 call within specific accuracy and reliability parameters. Since the industry has largely migrated to Phase II, only Phase II scenarios will be addressed in this Report.

To fulfill Phase II requirements for the delivery of latitude and longitude associated with the 9-1-1 call, CMRS carriers have deployed location determination technologies in their networks. The location technologies may be handset-based (e.g., Assisted Global Positioning System [AGPS]) or network-based (e.g., Time Difference of Arrival [TDOA], Angle of Arrival [AOA], etc.). However, due to limitations in some location determination technology that result in delays in obtaining Phase II location, existing Phase II implementations route emergency calls using a location key, derived based upon the cell site on which the call originated, that is communicated via call setup signaling. Phase II location information is delivered over a separate data link between the CMRS network and the Emergency Services Network. The E2 protocol defined in J-STD-036-C and NENA-05-001 is typically used over the data link between the CMRS network and Emergency Services Network to request/deliver initial caller location information to the PSAP via the ALI system, and to provide updated location information when requested.

There are two variants of the approach to acquire Phase II location: one is referred to as Non-Call Associated Signaling (NCAS) and the other is referred to as Wireline Compatibility Mode (WCM). Of the two variants, the WCM approach is more widely deployed and is the only one discussed in this Report.

With the WCM approach, Phase II location information and the callback number are sent over a separate data link to the ALI database from the Mobile Positioning Center/Global Mobile Location Center (MPC/ GMLC) in the CMRS network. The Mobile Switiching Center (MSC) may support either an MF or an SS7 interface over which a single 10-digit number is delivered to the SR, and the SR supports an interface where only a single 7/10-digit number is delivered to the PSAP. The one piece of information sent by the MSC to the SR is referred to as the Emergency Services Routing Key (ESRK). The ESRK may represent the PSAP or an Emergency Service Zone (ESZ) in the jurisdiction of a PSAP, and also uniquely identifies the 9-1-1 call. The ESRK also uniquely identifies an MPC/GMLC in the CMRS network that the ALI database must query. The MPC/GMLC stores a pool of ESRKs in its database that represent a PSAP or ESZ and assigns them to wireless 9-1-1 calls. The PSAP receives only the ESRK from the SR and uses it to query the ALI database, which in turn queries the MPC/GMLC. The MPC/GMLC returns the callback number and the latitude and longitude information for the mobile caller.

So as shown in the figure below the legacy CMRS carrier’s network has an Signal System No. 7 (SS7) or multi-frequency (MF) interface to the SR. The parties must agree upon the connection method. When the CMRS customer initiates a 9-1-1 call, the ESRK is passed to the SR and the SR queries the SRDB to obtain the ESN associated with the ESRK. The SR then uses the ESN to determine the appropriate PSAP and delivers the call with the ESRK.

Also as shown in the figure below the legacy CMRS carrier has an interconnection to support the E2 interface. This interface is used to obtain the caller’s location. The parties must agree upon the connection method used to support the E2 interface. When the PSAP queries the ALI database with the ESRK, the ALI database steers the query to the MPC/GMLC. The MPC/GMLC returns the callback number and caller’s location to the ALI database, which in turn returns it to the PSAP.



##### Interim VoIP E9-1-1 Interconnection

Interim VoIP E9-1-1 makes use of a Validation Database (VDB) within the VoIP Service Provider (VSP) network to ensure that civic location information representing VoIP end user locations are MSAG valid. The VDB contains information that describes the current, valid civic address space defined by the E9-1-1 SSP MSAG. The MSAG must be provided to the VSP by the E9-1-1 SSP. To support emergency calling, VoIP customers’ location is managed by the VSP rather than the E9-1-1 SSP. This location information is provisioned to a system referred to as a VoIP Positioning Center (VPC) after being validated by the VDB.

Existing interim VoIP implementations use the wireless E9-1-1 WCM techniques described above as a basis for delivering emergency originations from VoIP callers to legacy PSAPs that are served by SRs. When a 9-1-1 call is initiated, the VPC allocates an Emergency Services Query Key (ESQK) to the call (in a manner similar to the way that an MPC/GMLC allocates an ESRK to a wireless emergency call). The ESQK identifies a call instance at a VPC, and is associated with a particular SR/ESN combination. The ESQK is delivered to the SR (without a callback number) via an Emergency Services Gateway (ESGW) over an MF or SS7 interface. The SR then queries the SRDB using the ESQK to determine the route (i.e., trunk group) to the target PSAP. The SR delivers the ESQK to the PSAP via MF signaling. The PSAP uses the ESQK to query the ALI system, and the ALI system steers the query back to the VPC (in the same manner as it would steer a query to an MPC/GMLC for a wireless emergency call). The VPC responds with the provisioned location information and a callback number. The ALI system then passes the location and callback information to the PSAP.

As shown in the figure below, the Emergency Services Gateway (ESGW) in the VSP network has an SS7 or MF interface to the SR. The parties must agree upon the connection method. When the VSP customer initiates a 9-1-1 call the ESQK is passed to the SR and the SR queries the SRDB to obtain the ESN associated with the ESQK. The SR then uses the ESN to determine the appropriate PSAP route/trunk group and delivers the call over that route/trunk group to the PSAP with the ESQK.

Also as shown in the figure below the VSP network has an interconnection to support the E2 interface. This interface is used to obtain the caller’s location. The parties must agree upon the connection method used for the E2 interface. When the PSAP queries the ALI database with the ESQK, the ALI database steers the query to the VPC. The VPC returns the call back number and caller’s location to the ALI database, which in turn returns it to the PSAP.

In order to keep the VSP MSAG copy accurate, the E9-1-1 SSP must periodically send to the VSP a complete MSAG file or a file containing the changes to the data (i.e., a delta file). The E9-1-1 SSP must have the necessary infrastructure to ensure the MSAG data is kept current and that updates are made available in an electronic form to the VSP in a timely fashion.

If validation errors occur, the VSP will only submit validation discrepancies to the E9-1-1 SSP after researching the issue and determining that the discrepancy can only be resolved by action on the part of the E9-1-1 SSP or the 9-1-1 Authority (i.e. update of the MSAG for new street addresses). This process must be negotiated between the VSP and the E9-1-1 SSP.



##### Legacy Small Cable Operators

Small cable operators have two options to interconnect to E9-1-1. The first is to operate as a small wireline carrier (i.e. a CLEC) as discussed in Section 5.1.1.1.1. The other option is to interconnect via a third party Interconnected VoIP Service Provider as discussed in Section 5.1.1.1.3. The predominate method of interconnection is the later where a third party operates as the VSP. Similarly to the discussion in Section 5.1.1.1.3, the small cable operator would send its customer callback information and address to the third party operator. That third party would validate the address and provision it in a VPC. At call time the small cable operator would send the 9-1-1 call to the third party operator which would route it to the emergency services network in a similar manner as discussed in Section 5.1.1.1.3.

#### Originating Service Provider IP Interconnection for NG9-1-1

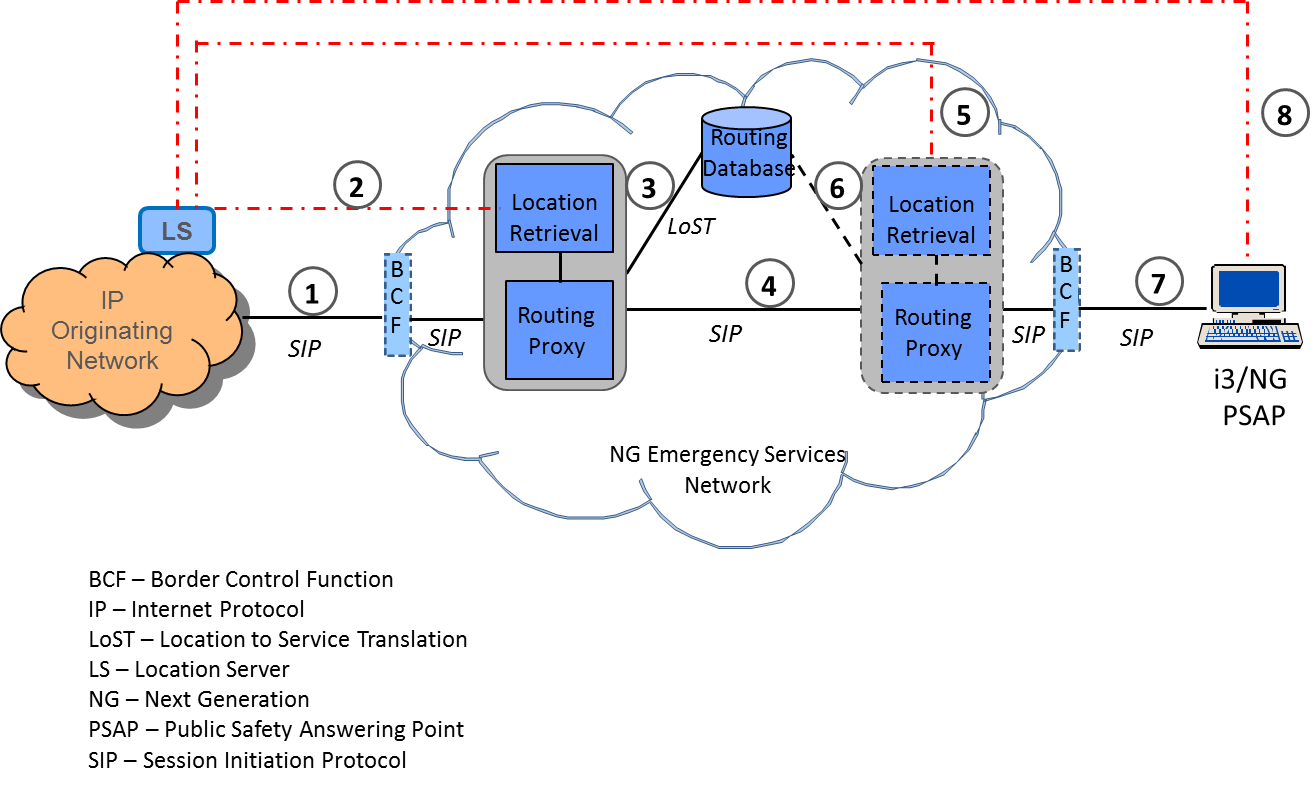
How small carriers interconnect with a NG Emergency Services Network depends upon the capabilities of the small carrier and considerations regarding the method of interconnection. If the small carrier has deployed an all-IP network it may interconnect with the NG Emergency Services Network via IP (i.e. using the SIP protocol). If the small carrier has not deployed an IP infrastructure then the small carrier must deliver the emergency call to a gateway that then interworks with the NG Emergency Services Network. This functional element is called a Legacy Network Gateway (LNG). As discussed below there are considerations related to the ownership of the LNG that impact financial and operational aspects of the small carrier deployment.

Two scenarios will be discussed. The first is where the small carrier interconnects with the NG Emergency Services Network using IP connectivity. The other is where the small carrier provides legacy connections (e.g. SS7 supported trunk groups) to the LNG. The implications of LNG ownership are also discussed.

##### IP Interconnection to an Next Generation (NG) Emergency Services Network

The following figure appears as Figure 5.1 in ATIS-0500034 *Comparison of Enhanced 9-1-1 (E9-1-1) and Next Generation 9-1-1 (NG9-1-1) Focused on Reportable Outage Data Points*. It illustrates interconnectivity for an all-IP NG9-1-1 system. This section will focus on steps 1 and 2. (Interconnection points 5 and 8 can be extrapolated from this discussion.) Interconnection point 1 is the signaling connection between the networks. Interconnection 2 is the dereferencing interconnection that may be used to acquire caller location.

While the figure does not illustrate media interconnectivity, media will go through a Border Control Function (BCF) in the IP Originating Network (not shown) to the ingress BCF in the NG Emergency Services Network. As small carriers initially migrate to support NG9-1-1 they will incorporate only the media type of voice. As they deploy text (e.g. Real Time Text [RTT]) and potentially video into their networks they may support delivering multimedia emergency calls to the emergency services networks. Interim Text (i.e. SMS to 9-1-1) is not considered NG9-1-1 and is not discussed in this Report.



1. The emergency call/session request is delivered by the IP originating network (via a Border Control Function) to a routing proxy in the NG Emergency Services Network with callback information and location information.

* Location may be delivered “by-value” (i.e., the civic location/street address or geo-coordinate location is contained within the SIP signaling message).
* Location may be delivered “by-reference” (i.e., the SIP signaling message contains a “pointer” or “reference” to the location information that includes the address of the element from which the location information can be obtained and a “key” to the data).

1. If the location information is received “by-reference”, the location retrieval functionality within or accessible to the routing proxy will be invoked.

* A dereference request will be sent to the element identified in the location reference (i.e., the Location Server [LS]) to obtain a routing location for the call.

If location is received “by-value”, this step will be omitted.

###### Considerations for Interconnection

In general, the NG9-1-1 SSP will identify two or more Point of Interconnections (POIs) for a given service. And as shown above there must be POIs for signaling and for location/data dereferencing. For signaling it is expected that the NG9-1-1 SSP will specify its POI at the ingress of the BCF[[20]](#footnote-20). The Small Carrier may be asked or expected to deliver its traffic to this POI. How it does that is based upon implementation decisions. For example, the connection could be a direct connect fiber connection. The small carrier may have implemented an IP network (e.g. using Multiprotocol Label Switching [MPLS]) that will deliver traffic to the POI. The data connection generally uses Hypertext Transfer Protocol (HTTP) signaling over IP. The small carrier may use similar methods to connect to the dereferencing POI. From a cost perspective, the small carrier may provide the transport facilities to the POI of the NG9-1-1 SSP and has options as to the most cost effective method to do so.

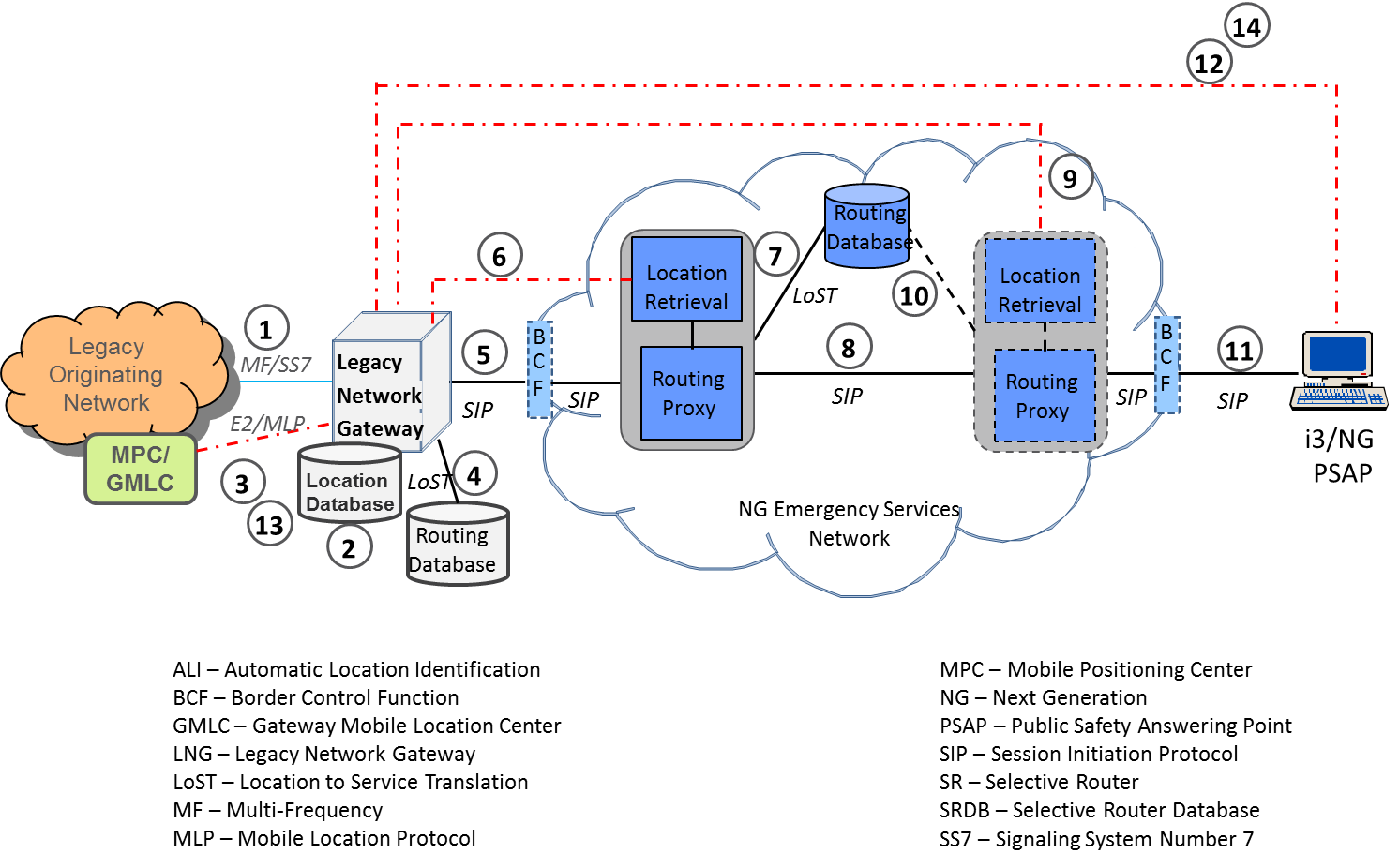
##### Transitional Interconnection to an NG Emergency Services Network

Although NG9-1-1 is defined to utilize an end-to-end IP architecture, there will continue to be legacy wireline and wireless (circuit switched) originating networks deployed after emergency service networks and a significant number of PSAPs have evolved to support NG9-1-1 architectures. Since any PSAPs served by NG Emergency Services Networks will need to be able to receive emergency calls that originate on these legacy networks, gateway functionality will be a required part of an NG9-1-1 Service Architecture. This gateway functionality must include signaling interworking to convert the incoming MF or SS7 signaling generated by a legacy origination network to the IP-based (i.e., SIP) signaling supported by an NG Emergency Services Network. In addition, since routing within the NG Emergency Services Network will be based on location, a gateway element on the ingress side of an NG Emergency Services Network must support the ability to use the information provided by a wireline switch or MSC in call setup signaling (e.g., calling number/ANI, ESRK, cell site/sector represented by an ESRD) to retrieve location information that can be used as input to routing determination. Based on the routing location provided, the routing determination function will identify which NG Emergency Services Network should handle the call. Routing location will also be used to support routing within the NG Emergency Services Network. Gateway functionality will also be needed to enable interactions between NG Emergency Services Network elements (and the PSAPs they serve) and legacy systems, such as MPCs/GMLCs, to support the retrieval of caller location to support the dispatch of emergency personnel.

To support emergency calls that originate in legacy networks, the NENA i3 Solution and ATIS IMS-based NG9-1-1 Service Architecture include the Legacy Network Gateway functional element. From the standards perspective, the LNG logically resides between the originating network and the NG Emergency Services Network and allows PSAPs served by the NG Emergency Services Network to receive emergency calls from legacy originating networks. The LNG provides protocol interworking from the SS7 or MF signaling that it receives from a legacy originating network to the SIP signaling used in the NG Emergency Services Network. In addition, the LNG is responsible for routing emergency calls to the appropriate element in the appropriate NG Emergency Services Network.

The Location Database associated with an LNG must support mappings from a specific calling number/ANI or pANI (e.g., ESRK, ESRD) value to a location that will result in the emergency call being routed to the target PSAP associated with the calling number/ANI/pANI. In addition to identifying the location to be used for emergency call routing, the LNG is also responsible for providing caller location to PSAPs for emergency calls that originate in legacy networks. The mechanisms used by an LNG to access caller location are comparable to those used by an ALI system to provide dispatch location to a PSAP in an E9-1-1 environment (i.e., by accessing provisioned data and steering queries to MPC/GMLCs in wireless originating networks, as appropriate).

Figure 5.2 from ATIS-0500034 shown below provides a high-level architecture diagram illustrating how emergency calls are processed using an interworking architecture involving an LNG. Interconnections points 1 through 6 and 13 will be discussed in this section. (Note that interconnection points 9, 12, and 14 can be extrapolated from this discussion.)



1. A 9-1-1 call is delivered by the legacy originating network to a Legacy Network Gateway (LNG) over an MF or SS7 trunk group.

* Legacy wireline originations are delivered with the SS7 Calling Party Number or MF ANI.
* Legacy wireless originations are delivered with an ESRK as the SS7 Calling Party Number or MF ANI, or with the Mobile Directory Number as the SS7 Calling Party Number/MF ANI and an ESRD/ESRK in the SS7 Generic Digits parameter/MF called number.

1. The LNG will interact with a local Location Database which will map the calling number/ANI/ESRK/ESRD to a routing location.
2. If the call is a legacy wireless emergency call, the LNG will also send an E2 or MLP query to the MPC/GMLC in the legacy wireless network requesting initial caller location.

* The location query will include the ESRK or MDN + ESRK/ESRD.
* The response from the MPC/GMLC will include initial (typically Phase I) caller location information.

1. The LNG queries a routing database using the routing location obtained in Step 2.

* The LNG queries the routing database with the routing location and an appropriate service URN.
* The routing database provides the address of a routing proxy in the NG Emergency Services Network.

1. The emergency call is delivered by the LNG (via a Border Control Function) to a routing proxy in the NG Emergency Services Network with a callback number and location information.

* If the call is a legacy wireline emergency call, the location obtained in Step 2 will typically be delivered “by-value” and will be in the form of a civic location/street address.
* If the call is a legacy wireless emergency call, the location will typically be delivered “by-reference” to allow location updates associated with the mobile caller to be requested.

1. If present in the call path, the routing proxy will use the location information received in incoming SIP signaling (location-by-value) or obtained by dereferencing a location-by-reference, and a service URN, to query a routing database using the LoST protocol.
2. If the location dereference request from the i3/NG PSAP indicates that initial location should be returned, the LNG will return the initial caller information obtained in Step 3. If the location dereference request from the i3/NG PSAP indicates that updated location should be returned, the LNG will send an E2 or MLP query to the MPC/GMLC requesting updated (i.e., Phase II) location.

While the LNG logically resides between the originating network and the NG Emergency Services Network, the function could be implemented by either the Originating Services Provider or the NG9-1-1 Service Provider (the concept of a third party is not discussed here). However, statutory, regulatory, costs, potential cost-recovery, rate-making, and universal service considerations could be huge determining factors on the approach to be taken in given areas.

###### Small Carrier Hosts the LNG

If the small carrier hosts the LNG, then interconnection points 1 through 4 and 13 are within the internal implementation of the small carrier. That is, the small carrier would interconnect to the LNG (e.g. via its own SS7 network) (1), validate and cache its customer location data (2), obtain the caller location during or subsequent to the call (3) and determine the destination NG Emergency Services Network (4). The small carrier would deliver the emergency call to the NG Emergency Services Network (using SIP) (5). In addition, the small carrier would provide a dereferencing interface (6) that may be used to access its internal Location Databases (2) to provide initial location or location updates.

In this scenario the small carrier must provide all of the functionality of the LNG, and offer the emergency call to the NG Emergency Services Network using native SIP. This scenario does not view the LNG as an aggregation point for multiple carriers and each small carrier must implement and deploy the LNG in order to connect to the NG Emergency Services Network.

###### NG Emergency Services Network Provider Hosts the LNG

If the NG Emergency Services Network Provider hosts the LNG, then interconnection points 1 and 3 and interface to the Location Database to provide customer location (2) are applicable to interconnections by the small carrier. Access to Interconnection point 2 means that there must be an agreement between the small carrier and the NG Emergency Services Network Provider such that the small carrier provides location information that can be validated and provisioned into the Location Database. For legacy wireless calls there may be a dereferencing interface (3) that could be used to query for the mobile caller’s location and used for location updates. The small carrier would deliver the emergency call (1) using legacy protocols, e.g. SS7, to the LNG. And the TN or pANI (ESRK or ESQK) would be provided in the calling party number.

In this scenario, the NG Emergency Services Network Provider hosts the LNG and the small carrier provides interconnection via legacy protocols. The NG Emergency Services Network Provider manages the interworking between legacy modes and those required by the NG Emergency Services Network. This scenario allows the LNG to be used as an aggregation point for multiple small carriers.

###### Hosting the LNG

If each small carrier was required to host the LNG, then their ability to offer emergency calls to the NG Emergency Services Network would be based upon their ability to fund and deploy the LNG. If the NG Emergency Services Network Provider hosts the LNG, then it can provide the LNG as a service and accommodate small carriers coming on board with minimal expense to the smaller carrier. There would need to be service agreements that would cover the interconnection and management of the location data into the Location Database.

### Call and Data Related Matters

In the E9-1-1 landscape, originating service providers send 9-1-1 calls to the 9-1-1 SSP portion of the E9-1-1 system, via trunk groups terminating at the SR which serves the geography of the subtending PSAPs (see Section 5.1.1 above). This may be done through direct trunking from the originating switches, or via intermediate third party transport providers. In addition, data describing their customers and service locations are provided to the 9-1-1 SSP for processing into routing control and location identification databases, which then direct calls to the appropriate PSAPs and supply the ALI data to the calltaker screens when a 9-1-1 call occurs. As such, the originating carrier has to be equipped to support these functions.

With NG9-1-1, the specifics change, but the basic functions required of a small carrier are similar. For transitional NG9-1-1, legacy trunking is still involved, but provided into legacy network gateways (LNGs – discussed in Section 5.1.1.2.2 above) either directly from the carrier or via third party transport providers. The LNG brings the traffic into the NG9-1-1 Core Services system via the ESInet, with firewall and security protections, so that the Routing Proxy can determine routing actions, based on GIS and Policy Routing information. The design of NG9‑1‑1 is IP-based, and both call and data flow are intended to flow across IP interfaces, including IP transport from carriers to the NG9-1-1 systems. As the date of this Report, that interface has been defined in ATIS standards (ATIS-0700015 [ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination](https://www.atis.org/docstore/product.aspx?id=28393)), but not yet implemented in real world service. That legacy to IP transition for transport will occur, but until it does, certain capabilities built into NG9-1-1 will be restricted. With both legacy and IP interfaces, certain data provisioning and validation actions are needed, based on data provided by the originating carrier or associated third party vendors the carrier may involve to support their roles. For wireless 9-1-1, the process is somewhat different, with special arrangements using MPC/GMLC operators to handle initial routing and ALI data flow into the central E9-1-1 or NG9-1-1 core services and on to the PSAPs.

#### LIS and LVF Validation Provisioning

The GIS data in NG9-1-1 Core Services is the basis for the Location Validation Function (LVF), which verifies that addressing and location data to be provided by originating entities are valid for 9‑1‑1 purposes. The preparation of the GIS data and its maintenance is a large and complex process, typically generated through local and state GIS organizations, in concert with PSAP managers, any PSAP and 9-1-1 Authorities Database groups, and the 9-1-1 SSP. Once it is established, location data in or intended for Location Information Servers (LIS) is compared through mechanized means with the LVF content. Any discrepancies are coordinated between originators and NG9-1-1 GIS groups as needed, resolved, and re-verified.[[21]](#footnote-21)

The LVF may be operated by the 9-1-1 Authority, or a separate LVF may be operated by the originating service provider, a set of originating service providers as a multi-entity service, or by a third party vendor employed by any of the above entities. In any case, the source of GIS data is derived from the `master’ GIS dataset associated with the NG9-1-1 Core Services process.[[22]](#footnote-22) Small carriers will need to coordinate the above process with the appropriate 9-1-1 Authorities and NG9-1-1 SSP entities.

#### Originating Service Provider Issues and Concerns

A critical issue for small carriers is the means by which caller location is supported for 9-1-1 calls. Caller location capabilities depend on what type of service is involved. Wireline and fixed VoIP services can and must provide caller location by telephone number, in today’s environment. Nomadic services should automatically provide caller location, but current practice is to require the customer to populate their info through a service provider website, typically, and update it when they move to another location, which is problematic. The service provider then supplies that data to the 9-1-1 process, as described above. Mobile services, including but not limited to CMRS providers, must arrange for MPC/GMLC services to support the identification of caller location estimates as the call progresses by leveraging many diverse technologies, e.g.,, device provided location, wifi access point sensing, and crowd sourcing methods. There are various standards developed by ATIS, NENA, and others, as well as specific requirements defined by the FCC for wireless 9-1-1 location.

In the near future, issues involving the support of Real Time Text (RTT) by carriers, multimedia including pictures and video from Smartphones, and many other types of data will have to be addressed. These all require IP transport, and the pressure to support IP end-to-end will affect small carriers and their capabilities and service support.

### Security

#### NG 9-1-1 Cybersecurity Considerations

As small carrier 9-1-1 networks transition from TDM-based to IP-based architecture, as part of the migration to NG9-1-1, they will face increasing exposure to cyber threats and vulnerabilities that did not exist in the legacy 9-1-1 environment. The strategy of any cybersecurity framework is rooted in the ability to identify assets, owners of these assets, threats/risks to these assets, and methods to mitigate the threats/risks. The human factor is also vital when preparing for and defending against cyber threats. Much of the proposed cybersecurity strategy in this Report is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NCF); National Initiative for Cybersecurity Education (NICE) framework for Cybersecurity education[[23]](#footnote-23); the ongoing work of the CSRIC; and current work either recently completed or underway from other authorities including the U.S. Department of Homeland Security (DHS).

The overall approach to NG9-1-1 network security must include small carriers. Cyber risk management strategies must be implemented while still taking into consideration available resources and levels of expertise. This part of the Report includes several sections; each intended to share specific information and recommendations to the small carrier community. The intent of this report is to provide recommendations for further study and to define core cybersecurity services that relate directly to the public safety and emergency communications enterprise, including both current legacy and future NG9-1-1 systems.

When reviewing these recommendations, readers should recognize that not every small carrier will have the same needs, capabilities or requirements, from either a personnel or network perspective. With this in mind, it is important to note that there are a number of deployment options available to carriers at a local operations level. It is neither reasonable, nor expected, that each small carrier nationwide would be able to implement every core cybersecurity service, hire cybersecurity experts, and/or provide their own in-house version of those suggested core services. Instead, cybersecurity core services, training and capabilities will likely be a combination of the most economic, technologically sound and operationally effective technologies available. It is the intent of CSRIC to provide options and information so that small carriers can make intelligent choices, from the available options, based on their local needs and capabilities.

#### Recommended Practices

##### Cybsecurity Workforce Development

One of the first recommended cybersecurity practices for small carriers during the NG9-1-1 transition is to prepare their workforce. This includes identifying the team responsible for protecting the NG9-1-1 ecosystem, clarifying roles, training the team and updating job descriptions.

The size of the team is relative to the size of the company and NG9-1-1 infrastructure being protected. Many small carriers will not have sufficient resources to dedicate internal staff members fully to cybersecurity or to hire external expertise. For this reason, it is important that the internal team represent diverse backgrounds. In addition to the technical expertise required for supporting the NG9-1-1 infrastructure, there should be representation from staff with responsibilities in corporate management, human resources (including safety), information technology, facilities management and public relations.

Once the team is established, it will be important to clarify the roles of the team members in regards to securing the NG9-1-1 ecosystem. Some team members will have technical responsibilities for securing the hardware, software and network connectivity of the ecosystem. Others will have non-technical responsibilities such as procuring training, updating job descriptions, working on vendor/supplier agreements, understanding regulations and drafting policies and procedures.

Once the roles are defined, the members of the team will need to identify training and education needed to prepare for their cybersecurity responsibilities. For the technical members of the group, this would include technical training (with an emphasis on cybersecurity) related to firewalls, session border controllers, switches, routers, servers and SIP trunking. The non-technical members of the group should focus their training on risk management, incident management, local/state/federal regulations and overall organizational awareness.

Job descriptions should be reviewed and updated to include cybersecurity responsibilities as well as knowledge and skill qualifications.

##### National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership among government, academia and the private sector that seeks to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our nation secure and economically competitive. The Workforce Framework lists and defines specialty areas of cybersecurity work and provides a description of each. Each of the types of work is placed into one of seven overall categories. The Workforce Framework also identifies common tasks and knowledge, skills and abilities (KSA's) associated with each specialty area.[[24]](#footnote-24)

Organizations or sectors can use the NICE Framework to develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training and education. A comprehensive application of the Workforce Framework is beyond the scope of this Report.[[25]](#footnote-25)

##### NIST Cybersecurity Framework (NCF)

The NCF is a voluntary framework developed by NIST, working with various stakeholders to identify existing standards, guidelines and practices that could be integrated into a guiding framework for reducing cyber risks to critical infrastructure. The framework core describes a set of activities that can be used to achieve the desired cybersecurity specific outcome. These activities are comprised of Functions, Categories, Subcategories and Informative References described below:

**Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome categories within this function include: Asset Management; Business Environment; Governance; Risk Assessment; Risk Management Strategy; and Supply Chain Risk Management (pending NIST 1.1).

Within the realm of a NG9-1-1 ecosystem, the small carrier should make a high level diagram of their NG9-1-1 environment and then inventory all hardware, software, suppliers and physical assets. Each NG9-1-1 asset should be assessed relative to the following characteristics:

1. Does the asset or supplier host sensitive NG9-1-1 data?
2. Is the integrity of the asset important so it cannot be changed either maliciously or accidentally to disrupt the NG9-1-1 ecosystem?
3. Does the NG9-1-1 ecosystem depend on the availability of the asset or supplier in order to handle emergency functions?

The risk assessment should consider the vulnerabilities of each small carrier asset in the NG9‑1‑1 ecosystem and weigh the likelihood and impact for each vulnerability. Suppliers to the NG9-1-1 ecosystem should also be contractually obligated to demonstrate their cybersecurity methodologies and quantify their cyber insurance indemnification limits.

**Protect** – Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome categories within this function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Some specific examples relative to protect functionality within the NG9-1-1 ecosystem include but are not limited to:

1. Awareness training should be provided to all employees and suppliers. More specific training should be provided to those who have direct responsibilities for securing the equipment supporting NG9-1-1 ecosystem.
2. Company processes and procedures related to cybersecurity should be clearly documented and shared with employees and suppliers.
3. Physical access to facilities housing small carrier assets associated with the NG9-1-1 ecosystems should be restricted to only those who need access through the use of an access control system. Surveillance and logging should be incorporated into those facilities.
4. Unique credentials with strong passwords should be issued for employees and suppliers. Credentials should only allow the bare minimum access privileges needed to support the NG9-1-1 ecosystem. Two-factor authentication should be considered for external access to systems. System access logs should be maintained for all activity. Credentials should be disabled as employees leave the organization.
5. Firewalls and Session Border Controllers should be used to protect NG9-1-1 related resources.
6. SIP trunks should be protected.
7. Access control lists should be incorporated within small carrier network devices to blacklist potential malicious access or more preferably whitelist valid access.
8. Firmware and operating system release levels should be kept current and consistent within the various components of the NG9-1-1 ecosystem.
9. Sensitive data in transit and at rest should be encrypted.
10. Configuration data and application data should be backed up on a regular interval which corresponds to the risk tolerance of data loss.

**Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome categories within this function include: Anomalies and Events; Security Continuous Monitoring and Detection Processes.

Some specific examples of NG9-1-1 detect functions include but are not limited to the following:

1. Employee awareness and defined procedures for reporting suspicious activity.
2. Alerts when physical or virtual access is attempted into the facilities supporting NG9-1-1, devices or software systems.
3. Alerts when unusual or excessive traffic patterns are detected within the NG9-1-1 ecosystem.
4. Regular review of log files of NG9-1-1 ecosystem devices.
5. Intrusion detection systems.

**Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation and Improvements.

Some specific examples of respond functions within the NG9-1-1 framework include:

1. Identifying the internal and external points of contact for the various types of incidents. If the incident results in an outage or impairment, the NG9-1-1 contact list could include the local PSAPs, regional or statewide 9-1-1 Authority and FCC Network Outage Reporting System (NORS).
2. Creating an incident response plan.
3. Testing the incident response plan.

**Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome categories within this function include: Recovery Planning; Improvements and Communications.

Some specific examples of recover functions with the NG9-1-1 framework include:

1. Redundancy and continuity planning and testing.
2. Testing backups and the ability to restore configuration and application data resulting from a cyberattack.
3. Post incident walkthrough meetings with the internal cybersecurity team to identify lessons learned.

In March 2015, the CSRIC IV published a document providing implementation guidance to help communication service providers use and adapt the voluntary NIST Cybersecurity Framework. This document can be found at: <https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf>.

##### DHS NG9-1-1 Resources

The DHS offers a number of optional programs and solutions for consideration by the public safety community. While the following is included in the report, it does not represent an endorsement of any specific program or project.

**Assessment and Analysis -** The DHS Office of Emergency Communications has published a specific report which is useful in identifying cyber risks specific to NG9-1-1. The report is located at the following DHS site:

[https://www.dhs.gov/sites/default/files/publications/NG9-1-1%20Cybersecurity%20Primer%20041216%20-%20508%20compliant.pdf](https://www.dhs.gov/sites/default/files/publications/NG911%20Cybersecurity%20Primer%20041216%20-%20508%20compliant.pdf).

This report can be a helpful resource when trying to navigate through the NIST framework within the scope of the NG9-1-1 ecosystem.

The Department has published the DHS Internet Protocol (IP) Emergency Services Sector Cyber Risk Assessment[[26]](#footnote-26) and Emergency Services Sector Roadmap to Secure Voice and Data Systems[[27]](#footnote-27) which provide pertinent guidance for public safety agencies, including those considering the adoption of NG9-1-1 technology and systems to strengthen their systems and networks against cyber risk through mitigation measures.

**Cybersecurity Operations -** The National Cybersecurity and Communications Integration Center (NCCIC) is a 24/7 cyber monitoring, incident response and management center. NCCIC/National Coordinating Center for Communications (NCCIC/NCC) is the federal lead organization for coordination of the Stafford Act’s National Response Framework ESF-2 (Communications) and is also the Communications Information Sharing and Analysis Center (ISAC), with cleared industry representatives from APCO, NENA and major carriers such as AT&T, Verizon, CenturyLink, Sprint and T-Mobile. Organizations can leverage NCCIC’s United States Computer Emergency Readiness Team (US-CERT) for cybersecurity information and assistance. Incidents can be reported at 1‑888‑828‑0870 or www.us-cert.gov/report.

US-CERT hosts the National Cyber Awareness System (NCAS), which offers a free, publicly available set of cybersecurity data including emerging threat data, alerts and reports.[[28]](#footnote-28)

**Public/Private Collaboration -** The Critical Infrastructure Cyber Information Sharing and Collaboration Program (CISCP) establishes trusted cyber information sharing relationships across Government and Industry. The CISCP facilitates the secure exchange of cybersecurity indicators, enabling organizations to protect themselves against emerging attacks. Currently, the CISCP has more than one hundred member organizations and is working in collaboration with the NCCIC to automate cybersecurity information sharing amongst its members.[[29]](#footnote-29)

**User Training and Education -** The DHS provides resources for cybersecurity training and awareness for use by any public or private entity. These resources can be leveraged to provide users with a basic level of awareness of cybersecurity risks. In many instances, cyber threat actors exploit untrained individuals (e.g., phishing attacks) to gain initial access to the enterprise and initiate further actions. The “Stop.Think.Connect. Campaign” is geared to provide awareness.[[30]](#footnote-30) The DHS also supports the National Initiative for Cybersecurity Education (NICE), which provides additional educational resources for public and private organizations.

**Outreach and Assistance -** The Critical Infrastructure Cyber Community C³ (pronounced “C Cubed”) Voluntary Program (C3VP) supports organizations of all sizes to establish or improve their cyber risk management processes and to take advantage of free technical assistance, tools and other resources offered by the U.S. Government. C3VP can assist small carriers in understanding how to use NIST’s Cybersecurity Framework and other risk management efforts.

**Technical Solutions -** The DHS offers a collection of programs and initiatives that can be applied to reduce NG9-1-1 cyber risks. Many of these efforts support missions that cover State and local users, as well as public and private critical infrastructure entities.

### Potential State and/or Federal NG9-1-1 Regulatory Considerations

As noted earlier in the background section, historical state and federal statutes or regulations regarding TDM network interconnection to a legacy 9-1-1 selective router in a particular LATA by small carriers has often been based on the process for interconnecting with the largest ILEC in an area. In some states, OSPs may be reimbursed for E9-1-1 network and/or data costs. Under the 1996 Act, the FCC has set guidance and policies on TDM interconnection and numbering, and state public utility commissions often implement interconnection accordingly.[[31]](#footnote-31)

TDM-to-TDM interconnection has been the traditional interconnection scenario, and IP-based providers have had to convert their traffic to TDM in order to interconnect and exchange traffic with ILECs within the LATA involved, unless arrangements for exchange of traffic in IP have been made. As traffic exchange evolves into full IP traffic exchange, expectations and responsibilities may change. It is also uncertain how traffic will be exchanged in the NG9-1-1 environment, and whether jurisdiction over NG9-1-1 traffic exchange will be state, federal, or shared. With the inherent flexibility that IP-to-IP Interconnection provides, interconnection options may range from mirroring legacy TDM interconnection within a particular LATA, to the opposite extreme of a limited number of interconnection points nationwide. Because of the special circumstances that could be potentially associated with some small carriers whose end user customer retail rates may be regulated by state public utility commissions, any additional costs associated with NG9-1-1 changes may only be paid for in one of three ways: (1) by an increase in rates to retail end user customers, (2) by additional direct tariff charges to the 9-1-1 Authority from that small carrier, or (3) by other means authorized by a state. Moreover, depending on a state’s approach to implementing NG9-1-1, an NG9-1-1 Services Provider may need to support TDM interconnection within a particular LATA to two LNGs.

At different stages of transitioning to NG9-1-1, the NG9-1-1 elements that are funcationlly equivalent to those used to support MSAG validation, (e.g., the LVF and LIS) may generate cost and deployment issues that have to be addressed, unless goverened by requriements imposed by a jurisdictional agency.

As the service industry migrates to service offerings based on full IP, it is important for small carriers within that industry to coordinate the process with those 9-1-1 Authorities impacted by the migration, and address how they will interconnect with the NG9-1-1 systems involved. Any failure to communicate specific plans for migration at the earliest possible time may hinder progress, and there could be unnecessary regulatory proceeding delays. Accordingly, this Report delivers a readiness tool to help small carriers to assess their level of NG9-1-1 readiness. This readiness tool should help small carriers to ensure they understand what the 9-1-1 Authority, or the NG9-1-1 Services Provider may be asking the small carriers to change from the status quo and the potential cost considerations associated with the requested NG9-1-1 transition. This tool can also be used to communicate the small carrier’s migration plan and the status of its execution to all appropriate parties.

### Funding

Unfunded mandates potentially make it difficult for small carriers to continue to operate and provide service. Smaller ILECs may not be able to afford to upgrade those facilities and services required for NG9-1-1, as traditional wireline and wireless 9-1-1 cost recovery programs are being revised and USF recovery mechanisms are now being capped or fixed. Rural CLECs may have no recovery mechanisms. As reported in the FCC’s Ninth Annual Report to Congress on State Collection and Distribution of 9-1-1 and Enhanced 9-1-1 Fees and Charges,[[32]](#footnote-32) over half the states have statewide 9-1-1 funds, while other states have local 9-1-1 funding programs. However, these funds are generally created for funding public safety 9-1-1 system costs which can include the ESInet network, database and PSAP equipment.

A recent whitepaper by the Wireless Infrastructure Association (WIA) speaks to the point:

*The United States relies on the 49 million Americans living in rural areas for most of its food, energy and water. Yet while most Americans benefit from today’s advanced wireless networks that allow them easy access to their community and content, the most advanced technologies have not been widely deployed in rural communities. It is difficult for mobile operators to justify the low Return on Investment (ROI) based on the number of people living in those communities with so many demands elsewhere on limited capital budgets.[[33]](#footnote-33)*

As the paper further observes, this is critical to emergency communications.

*Because the overwhelming majority of Americans rely on wireless networks to contact public-safety personnel, it will be critical for people living in rural areas to have the wireless infrastructure necessary for next-generation emergency services to function. In addition to basic emergency services requested today via wireless devices (ambulance requests, police and fire calls, traffic accidents, reports of criminal activity, etc.) the future of wireless technology will provide a more robust suite of emergency services and safety features.[[34]](#footnote-34)*

The Commission is sensitive to these issues. Recently, following the Universal Service Administrative Company’s announcement that the budget control mechanism adopted in 2016 will cut universal service support for small, rural carriers by 15.52% over the course of the next year, FCC Chairman Ajit Pai noted that that mechanism --

*. . . has created constant uncertainty for small, rural carriers, endangering their ability to make long-term investment decisions to bring high-speed broadband to the millions of Americans who still lack it. That’s why earlier this year we allocated $180 million to such carriers as a stop-gap measure to avert budget cuts for the current funding year.[[35]](#footnote-35)*

This Report evaluates the issues for small carriers that are migrating to support NG9-1-1 and advises the FCC on small carrier issues related to NG9‑1‑1 implementation, including what economic disadvantages, if any, may impede small carriers in the implementation of NG9-1-1; and what barriers to implementation, if any, the FCC should address. Some state and local governments in a legacy 9-1-1 environment provided cost recovery programs for carriers establishing dedicated 9-1-1 networks for the purposes of 9-1-1 call routing, covered 9-1-1 database management expenses and partnered with the rural areas for the deployment of Enhanced 9-1-1 services. As State and Regional 9-1-1 Authorities modify cost recovery programs and remove reimbursement for rural carriers this could place the carrier in an economic disadvantage. State and Regional 9-1-1 Authorities are encouraged to understand the impacts of modifying cost recovery programs and remain flexible to address some of the economic issues impacting the carriers. State and Regional 9-1-1 Authorities may want to consider establishing a relationship with small carriers for the purpose of supporting NG9-1-1 implemenation and identifying potential funding gaps.

The National Emergency Number Association (NENA), in their document on “Potential Points of Demarcation in NG9-1-1 Networks Information Document” discussed “Policy and Financial Issues Regarding Demarcation of the LNG.”

*Configuration of demarcation for the LNG has some interdependencies with the rollout schedule for actually implementing the equipment. As of this writing, there exists no clear precedent for the migration path from an … SR(s)-only environment to one which uses LSRG(s) and/or LNG(s). ... Deployment of the LNG is currently an unknown cost in future NG911 networks. Demarcation is the primary catalyst for shifting cost towards either party, and as there exists no consensus for a single form of demarcation, there exists no clear guidance for determining the responsibility for funding the LNG. This would appear to call for the development and of regulations to establish standardized demarcation points and the respective roles and responsibilities of the parties.[[36]](#footnote-36)*

CSRIC recommends that the Commission explore opportunities to resolve cost recover debate, up to and including formal rule-making as appropriate. In May, 2001, for example, the Commission responded to a request from King County, Washington regarding funding of wireless network and database components, and established what is historically known as the “King County Ruling” whereby demarcation and cost recovery responsibilities were defined. Given the vast changes in technology since the Commission’s original wireless demarcation decision, it is critical that the ruling be revisited. Absent the Commission updating the King County Ruling to accommodate NG9-1-1 IP environments, exacerbates the debate of “who pays.”[[37]](#footnote-37)

### Other Issues and Factors

#### Transition Timelines

The small carrier transition timelines will vary by carrier depending on the resources they have available to focus on the transition. It is important that small carriers work with their state or regional 9-1-1 Authority to coordinate their transition timelines and expectations. One good source to help identify appropriate contacts for such authorities is the National Association of State 911 Administrators (NASNA).[[38]](#footnote-38) As the name implies, the Association serves directors of state level 9-1-1 programs. While state 9-1-1 program responsibilities vary from state to state, most state contacts will have familiarity with substate 9-1-1 Authorities and serving 9-1-1 jurisdictions; and, can help provide support and information regarding service provider/9-1-1 authority interconnection matters.

It is recommended that small carriers create an implementation plan. The implementation team should include a coordinator and key staff members who will be responsible for implementing and maintaining the carrier’s NG9-1-1 ecosystem. Some major milestones would include:

* Understanding the plans and timeline for the state/regional 9-1-1 Authority.
* Identifying the technology changes that need to be implemented on the network.
* Identifying organizational impact such as training and job duties.
* Understanding the interoperability requirements with the ESInet and other carriers.
* Budgeting for equipment, software, training, third party service, and other expenditures.
* Acquiring equipment, software and third party services.
* Executing training plans.
* Deploying equipment and software.
* Provisioning SIP trunks to the ESInet.
* Testing.
* Completing migration for support of NG9-1-1.

Small wireless carriers may need at least eighteen months, or much longer, to prepare staff, budget, acquire equipment, prepare and test their infrastructure to handle VoLTE (Voice over LTE) NG9-1-1 roaming and MMES (Multi-Media Emergency Service) NG9-1-1 capabilities.

Small wireline carriers may need at least eighteen months, or much longer, to prepare staff, budget, acquire, and implement SBCs (Session Border Controllers), provision diverse SIP trunks and test capabilities.

#### Devices

With the transition to NG9-1-1, there is the potential for greater diversity of devices initiating 9‑1-1 communications with the small carriers networks.

Small wireless carriers have no control over the device ecosystem, and are frequently last in line to gain access to network equipment, devices and handsets. Access to major device manufacturers typically start with the large carriers, and device interoperability available to small carriers for new or enhanced emergency alert functionality could be months or even years behind the larger carriers. Device operating sytems and updates are typically controlled by the manufacturer and subscribers are more capable of installing custom applications on the devices which could enhance or disrupt 9-1-1 functionality.

Although it is outside the scope for small carriers to anticipate and test every possible type of device that will be interacting with their network, it is recommended that carriers at least test the NG9-1-1 functionality of those devices that they are selling or providing to their subscribers.

#### Roaming Implications

For small wireless carriers, roaming interoperability between small carriers and Tier 1 carriers may be a challenge for handling NG9-1-1 calls.

Carriers may implement different Heighten Accuracy Location Information (HALI) solutions when providing emergency services and to meet the requirements such as the FCC’s Fourth Report and Order on Location accuracy. The ATIS-0700028 [*Location Accuracy Improvements for Emergency Calls*](https://www.atis.org/docstore/product.aspx?id=28273) standard defined methods and procedures to support HALI such as Dispatchable Location which requires devices to retrieve visible reference points (e.g., WiFi access points) to identify nearby civic addresses that can be used for emergency response.

The current ATIS-0700028 standard describes several means by which this information can be retrieved for LTE access: (1) control plane using LPP per 3GPP Release 13, (2) control plane using LPPe 1.0 per OMA, (3) user plane using SUPL (LPP) 3GPP Release 13, and (4) user plane using SUPL (LPPe) 1.0 per OMA. A carrier network or device can be compliant to the ATIS-0700028 standard by implementing any one of these methods.

Geodetic HALI implementation differences beyond dispatchable location, including Z-Axis technologies, may also exist between carriers.[[39]](#footnote-39) A given carrier may select one method to be used, while another carrier can select a different method to be supported. Further, a device OEM may implement one method, but this method may not be supported by all carriers that offer that device. Unfortunately, there is currently no guarantee that all carriers and all device OEMs will implement the same method. This may lead to interoperability issues when devices roam between networks.

For example, assume carrier A and device DA implement control plane LPP to retrieve the information and carrier B and device DB implement control plane LPPe. When device DA originates an emergency call while roaming in carrier B, carrier B will not be able to retrieve HALI from the device because the two methods are incompatible. The same would be true for device DB when roaming in carrier A’s network.

The implication for transition to supporting NG9-1-1 is that if the small carrier supports one method and a Tier 1 carrier supports another, the roamed-to carrier may not be able to achieve the same level of location accuracy performance. Differences in location latency given different implementation methods may also impact the ability to improve call routing beyond cell based routing.

As small wireless carriers transition their voice calls to VoLTE, interoperability can be a significant challenge. In addition to the technical issues discussed above, it can take six months or longer of testing per carrier for VoLTE roaming and NG9-1-1 interoperability between two carriers who have a desire to allow roaming.

#### Capacity Issues during Major Emergencies

NG9-1-1 presents a new array of capacity planning challenges for small carriers. Large data sizes, combined with the potential for high volume of MMEScalls, will need to be factored into sizing SIP trunks between the small carrier and the ESInet.

Small ILEC carriers may have PSAPs residing in their serving area in which the ILEC carrier is responsible for providing data connections and terminating voice services to the PSAP. In these situations, the ILEC carrier may need to work with the serving 9-1-1 Authority to provide adequate capacity for NG9-1-1 SIP trunks which may be terminating in their service area. Depending on the capacity requirements and potential for MMES growth, this could result in the need for fiber or equipment upgrades.

#### Staff Preparation

Below are some suggestions for small carriers to prepare their staff for the NG9-1-1 transition.

* Carriers should stay abreast of the NG9-1-1 transition to better understand the ecosystem, timelines, and implications for their companies.
* Carriers should establish contact with NG9-1-1 Authorities within their service areas and gather information such as implementation schedules and functionality expectations.
* Carriers should consider SIP training and best practices to enable their staff to provision reliable and secure SIP trunks.
* Carriers should prepare their staff for Cybersecurity issues related to NG9-1-1 as addressed in section 5.1.3.

## Small Carrier Readiness Checklist

As noted above, CSRIC was also asked to recommend a “NG9-1-1 readiness checklist” for small carriers analogous to the one the Commission’s TFOPA developed for PSAPs. In the TFOPA WG2 Supplemental Report, said Scorecard identified “essential elements” necessary during each stage of transition to NG9-1-1 for the PSAP community. As stated,

*The NG9-1-1 Readiness Scorecard provides a 9-1-1 Authority Stakeholder with a more granular understanding of essential NG9-1-1 system elements and enables a 9-1-1 Authority Stakeholder to assess their position within the NG9-1-1 Implementation Maturity Continuum. This understanding will allow a 9-1-1 Authority Stakeholder to better plan transition steps to move from legacy 9-1-1 through being in a fully functional NG9-1-1 end state. Additionally, by understanding essential NG9-1-1 system elements in each maturity state, a 9-1-1 Authority Stakeholder will be able to plan for and budget transition costs.[[40]](#footnote-40)*

The transition process followed a “maturity continuum” ranging from a “legacy state” through “foundational, transitional, and intermediate” stages, on the way to a goal of full “end state” NG9-1-1. Specifically, the Report defined “end state” as

*. . . the state in which PSAPs are served by i3 standards-based systems and/or elements, from ingress through multimedia "call" handling. Originating Service Providers are providing SIP interfaces and location information during call set-up time. Within the jurisdiction, ESInets are interconnected providing interoperability which is supported by established agreements, policies and procedures. Systems in the End State are NG9-1-1 Compliant.[[41]](#footnote-41)*

However, for originating service providers, being ready to support NG9-1-1 does not necessarily involve that many process “states.” CSRIC VI Working Group 1 reviewed the TFOPA report referenced above and identified those “readiness” stages the Working Group felt appropriate to small originating service providers, as described below.

### Stages of Readiness

The critical part of readiness for small originating service providers is that as they migrate their networks from legacy TDM signaling to IP-based network architectures they incorporate the capabilities required to interconnect with and support NG9-1-1. CSRIC VI Working Group 1 defined three stages of such support, ranging from current legacy support, through a transitionary phase, to full end-state NG9-1-1 support.

* **OSP Legacy**

The OSP Legacy stage is characterized as the point in time where 9-1-1 services are provided by the traditional E9-1-1 SSP (e.g. ILEC) with circuit-switched infrastructure and ALI circuits. And, the small carrier interconnects with public safety systems using legacy protocols. Section 5.1.1.1.1 discusses legacy wireline carrier interconnection. Section 5.1.1.1.2 discusses legacy small CMRS carrier interconnection. Section 5.1.1.1.3 discusses Interconnected VoIP carrier interconnection. Section 5.1.1.1.4 discusses small cable carrier interconnection.

* **OSP Transitional**

The OSP Transitional state is where the NG9-1-1 SSP has deployed aspects of NG9-1-1 as discussed in the Transitional State, Intermediate State or Jurisdictional End State as defined by the TFOPA Report.

In this state, the small carrier has not yet migrated to an IP-based network environment but is able to interconnect with the NG9-1-1 SSP’s ESInet. Two methods are discussed in this Report. Section 5.1.1.2.2 of this Report discusses options for the small carrier to interconnect to the ESInet using a LNG.

* Section 5.1.1.2.2.1 discusses the method where the small carrier provides the LNG. In this method the small carrier converts its TDM signaling to SIP and interconnects with the ESInet using native SIP. And the small carrier converts the legacy data access protocols (e.g. E2) to those used by NG9-1-1.
* Section 5.1.1.2.2.2 discusses the method where the NG9-1-1 SSP provides the LNG. In this method the small carrier interconnects with the NG9-1-1 SSP’s LNG using legacy signaling (e.g., TDM) and data access protocols (e.g., E2).
* **OSP NG9-1-1 End State**

The OSP NG9-1-1 End State is where the small carrier has deployed an IP-based network and the NG9-1-1 SSP has deployed aspects of NG9-1-1 as discussed in the Jurisdictional End State as defined by the TFOPA Report. The small carrier interconnects via native SIP and provides data access protocols used by NG9-1-1. This method is discussed in Section 5.1.1.2.1 of this Report.

### Essential Elements of Readiness

The Checklist below is organized around seven areas of readiness, including:

* Public Safety Governance and Regulatory Matters

How public safety 9-1-1 Authorities organize and design their systems can impact the matter in which service providers support the delivery and processing of 9-1-1 services. For example, such matters may involve the location and nature of points-of-interconnection, along with essential data matters. This element addresses that, along with other support features impacted by regulatory, service standards and funding.

* Routing and Location

Routing and location defines the systematic approach that is used to determine 9-1-1 call routing to the appropriate emergency services network, and the supporting data functions. Before the small carrier converts to an IP-based network, legacy 9-1-1 calls are processed using legacy methods (e.g,. by relaying the calling telephone number, the ESRK or ESQK to an LNG). The LNG routes the call to the ESInet and manages location information queries. When the small carrier supports NG9-1-1 capabilities, the small carrier network will utilize geospatial routing based on the caller’s location to determine the appropriate emergency services network. A “pure” or “end-state” NG9-1-1 implementation assumes OSPs have changed the means by which they deliver 9-1-1 calls, however it is not realistic or expected that all small carrier OSPs will change at the same time. Therefore, the model is complicated by mechanisms to “transition” from legacy methods to NG9-1-1 methods. The LNG is required until all OSPs deliver location information with their 9-1-1 call setup messages (location-by-value) or provide location databases that may be queried (location-by-reference). Nationwide OSPs will utilize a National Forest Guide to determine to which ESInet to direct a given 9-1-1 call.[[42]](#footnote-42) As discussed in the TFOPA Report, “Hierarchical Forest Guides Populated” indicates a provisioning capability for various Forest Guides to share the routing polygon (ESInet or PSAP Jurisdictional boundary) information.

* GIS Data

GIS Data is a fundamental element of NG9-1-1 but is not utilized for legacy 9-1-1 call routing. Small carriers will need GIS data provided by the 9-1-1 Authority, or access to it. The exchange of jurisdictional boundary information may require an automated mechanism where the GIS information automatically keeps a routing function updated with its jurisdictional polygons to allow for 9-1-1 call handling. GIS data may also be utilized within the small carrier (or with access to it) for the validation (LVF) function to support customer address validation.

* Network

The network area capabilities represent the various technology mechanisms for connecting small carrier networks to either a legacy SR or an ESInet for the purposes of processing 9-1-1 calls. Prior to the small carrier migrating to an IP-based network, legacy call circuit mechanisms are primarily TDM based technology (e.g., SS7, CAMA) and once the small carrier migrates to IP-based technology it introduces application specific protocols such as SIP and RTP (Real Time Transport Protocol). E2 circuits are the legacy wireless and Interconnected VoIP vehicles for retrieving location information and will be required until all small carriers allow location acquisition transactions to deliver the caller’s location information at call setup time.

* Security

Security includes capabilities, operations and best practices for the interconnection to the ESInet.

* Operational Planning

Operations planning addresses aspects of execution, oversight, plan management and efforts to support on-going evolution with the planning of connection to the ESInet and the transition to the NG9-1-1 processing model and services.

* Optional Interfaces

Optional Interfaces addresses services and interfaces that interconnect with the ESInet but apply beyond NG Core Services primary functions, although these functions may otherwise appear necessary and prudent. Any and all optional interfaces must comply with all applicable industry interface standards and shall not interfere with or impact the function or security of the NG9-1-1 systems.

Within each of these areas, “essential elements” of readiness are identified based upon the earlier sections of this report.

### Small Carrier Checklist

The following tables provide a checklist to support the transition of legacy 9-1-1 services to NG9-1-1 for a small wireline carrier (e.g. CLEC or Independent wireline carrier). The Table cells indicate the section within the Report that provides relevant information to the essential elements involved.

Table 3 Small Wireline Carrier Checklist

| **Small Carrier Checklist – Wireline Carrier** | | | |
| --- | --- | --- | --- |
| **Essential Elements of Readiness** | **OSP Stages of Readiness** | | |
| **Legacy** | **Transitional** | **End State**  **NG9-1-1** |
| **Public Safety Governance and Regulatory Matters** | | | |
| Interaction with serving 9-1-1 Authorities, and address regulatory matters as necessary |  | [5.1.4](#_Potential_State_and/or) | [5.1.4](#_Potential_State_and/or) |
| Transition strategies |  | [5.1.4](#_Potential_State_and/or) | [5.1.4](#_Potential_State_and/or) |
| Funding |  | [5.1.5](#_Funding) | [5.1.5](#_Funding) |
| Confirm interconnection via TDM or via IP-to-IP. | 5.1.1.2 |  |  |
| If TDM, verify whether the 9-1-1 Authority is planning to have the small carrier remain connected to the legacy selective router initially, and for how long. | [5.1.1.2](#_Originating_Service_Provider) |  |  |
| If TDM, verify the deployment of necessary LNGs (where are the LNGs proposed to be located, and where are the associated interconnection points) |  | [5.1.1.2.2](#_Transitional_Interconnection_to) |  |
| If IP-to-IP, determine if there is an IP-to-IP interconnection specifications document available and confirm the proposed points of IP-to-IP Interconnection. |  | [5.1.1.2.1](#_IP_Interconnection_to) | [5.1.1.2.1](#_IP_Interconnection_to) |
| Determine if the current 9-1-1 data process is initially expected to change, and confirm the timing of that process. |  | [5.1.1.2.1](#_IP_Interconnection_to) |  |
| Confirm the timing of transition to full i3 NG9‑1-1. |  |  | [5.1.1.2.1](#_IP_Interconnection_to) |
| In that context, compare the timing of the 9-1-1 Authority’s transition timeline in comparison to the carrier’s transition timeline towards IP transition, and reconcile any impact disparities that may generate. |  |  | [5.1.1.2.1](#_IP_Interconnection_to) |
|  |  |  |  |
| **Routing & Location** | | | |
| TN Routing | 5.1.1.1.1 | 5.1.1.1.1 |  |
| GIS Routing |  |  | 5.1.2 |
| Location in INVITE (LbyV) |  |  | 5.1.1.2.1 |
| Access to Forest Guide |  |  | 5.2.2 |
|  |  |  |  |
| **GIS Data** | | | |
| Access to GIS for validation |  |  | 5.1.2.1 |
| Access to GIS for routing |  |  | 5.1.2.1 |
|  |  |  |  |
| **Network** | | | |
| Interconnection Agreements | 5.1.1.1.1 | 5.1.1.1.1 | [5.1.1.2.1.1](file:///C:\Users\jgoer\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\CSRIC6-WG1-00070R000%20(1).docx#_Recommendations_on_Interconnection) |
| TDM-based Network | 5.1.1.1.1 | 5.1.1.1.1 |  |
| IP-based Core Network |  |  | 5.1.1.2.1 |
| LNG |  | [5.1.1.2.2.1](file:///C:\Users\jgoer\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\CSRIC6-WG1-00070R000%20(1).docx#_Small_Carrier_Hosts)  [5.1.1.2.2.2](file:///C:\Users\jgoer\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\CSRIC6-WG1-00070R000%20(1).docx#_NG_Emergency_Services)  [5.1.1.2.2.3](file:///C:\Users\jgoer\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\CSRIC6-WG1-00070R000%20(1).docx#_Recommendations_on_Hosting) |  |
| Location Validation (LVF) |  |  | [5.1.2.1](file:///C:\Users\jgoer\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\CSRIC6-WG1-00070R000%20(1).docx#_LIS_and_LVF) |
| LIS |  |  | 5.1.2.1 |
|  |  |  |  |
| **Security** | | | |
| Establish Cyber Team | [5.1.3.3.1](#_Cybsecurity_Workforce_Development) | [5.1.3.3.1](#_Cybsecurity_Workforce_Development) | [5.1.3.3.1](#_Cybsecurity_Workforce_Development) |
| Clarify Roles of Cyber Team | [5.1.3.3.1](#_Cybsecurity_Workforce_Development) | [5.1.3.3.1](#_Cybsecurity_Workforce_Development) | [5.1.3.3.1](#_Cybsecurity_Workforce_Development) |
| Identify Cyber Education and Training | [5.1.3.3.1](#_Cybsecurity_Workforce_Development) | [5.1.3.3.1](#_Cybsecurity_Workforce_Development) | [5.1.3.3.1](#_Cybsecurity_Workforce_Development) |
| Review Job Descriptions for Cyber Responsibilities | [5.1.3.3.1](#_Cybsecurity_Workforce_Development) | [5.1.3.3.1](#_Cybsecurity_Workforce_Development) | [5.1.3.3.1](#_Cybsecurity_Workforce_Development) |
| Inventory NG911 Hardware, Software, and Suppliers | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) |
| Assess sensitivity, integrity, and availability impact of NG911 Hardware, Software, and Suppliers | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) |
| Identify potential vulnerabilities of NG911 Hardware, Software, and Suppliers | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) |
| Develop and implement protective safeguards. | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) |
| Develop and implement functions to detect cybersecurity events. | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) |
| Develop a cybersecurity incident response plan. | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) |
| Develop cybersecurity incident recovery strategies. | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) | [5.1.3.3.3](#_NIST_Cybersecurity_Framework) |
| **Operations Planning** | | | |
| Interconnection Planning Procedures |  | [5.1.1](#_Interconnection) | [5.1.1](#_Interconnection) |
| Devlop Implementation Plan |  | 5.1.6.1 | 5.1.6.1 |
| Interconnection Monitoring Procedures |  | [5.1.1](#_Interconnection) | [5.1.1](#_Interconnection) |
| Staffing |  | 5.1.6.1 | 5.1.6.1 |
| Training |  | 5.1.6.1 | 5.1.6.1 |
|  |  |  |  |
| **Optional Interfaces** | | | |
| Additional Data Repository |  |  | Optional |
|  |  |  |  |

The following table provides a checklist to support the transition to support NG9-1-1 for small CMRS carriers (e.g. regional wireless providers). The Table cells indicates the section within the Report that provides relevant information.

Table 4 Small CMRS Carrier Checklist

| **Small Carrier Checklist – CMRS Carrier** | | | |
| --- | --- | --- | --- |
| **Essential Elements of Readiness** | **OSP Stages of Readiness** | | |
| **Legacy** | **Transitional** | **Legacy** |
| **Public Safety Governance and Regulatory Matters** | | | |
| Interaction with serving 9-1-1 Authorities, and address regulatory matters as necessary |  | 5.1.4 | 5.1.4 |
| Transition strategies |  | [5.1.4](#_Potential_State_and/or) | [5.1.4](#_Potential_State_and/or) |
| Funding |  | 5.1.5 | 5.1.5 |
| Confirm interconnection via TDM or via IP-to-IP. | 5.1.1.2 |  |  |
| If TDM, verify whether the 9-1-1 Authority is planning to have the small carrier remain connected to the legacy selective router initially, and for how long. | [5.1.1.2](#_Originating_Service_Provider) |  |  |
| If TDM, verify the deployment of necessary LNGs (where are the LNGs proposed to be located, and where are the associated interconnection points) |  | [5.1.1.2.2](#_Transitional_Interconnection_to) |  |
| If IP-to-IP, determine if there is an IP-to-IP interconnection specifications document available and confirm the proposed points of IP-to-IP Interconnection. |  | [5.1.1.2.1](#_IP_Interconnection_to) | [5.1.1.2.1](#_IP_Interconnection_to) |
| Determine if the current 9-1-1 data process is initially expected to change, and confirm the timing of that process. |  | [5.1.1.2.1](#_IP_Interconnection_to) |  |
| Confirm the timing of transition to full i3 NG9‑1-1. |  |  | [5.1.1.2.1](#_IP_Interconnection_to) |
| In that context, compare the timing of the 9-1-1 Authority’s transition timeline in comparison to the carrier’s transition timeline towards IP transition, and reconcile any impact disparities that may generate. |  |  | [5.1.1.2.1](#_IP_Interconnection_to) |
|  |  |  |  |
| **Routing & Location** | | | |
| pANI Routing | 5.1.1.1.2 | 5.1.1.1.2 |  |
| GIS Routing |  |  | 5.1.2 |
| Location reference in INVITE (LbyR) |  |  | 5.1.1.2.1 |
| Identify Location Acquisition Capabilities |  |  | 5.1.1.2.1 |
| Access to Forest Guide |  |  | 5.2.2 |
|  |  |  |  |
| **GIS Data** | | | |
| Access to GIS for routing |  |  | 5.1.2.1 |
|  |  |  |  |
| **Network** | | | |
| Interconnection Agreements | 5.1.1.1.2 | 5.1.1.1.2 | 5.1.1.2.1.1 |
| TDM-based Network | 5.1.1.1.2 | 5.1.1.1.2 |  |
| IP-based Core Network |  |  | 5.1.1.2.1 |
| LNG |  | 5.1.1.2.2.1  5.1.1.2.2.2  5.1.1.2.2.3 |  |
| **Security** | | | |
| Establish Cyber Team | 5.1.3.3.1 | 5.1.3.3.1 | 5.1.3.3.1 |
| Clarify Roles of Cyber Team | 5.1.3.3.1 | 5.1.3.3.1 | 5.1.3.3.1 |
| Identify Cyber Education and Training | 5.1.3.3.1 | 5.1.3.3.1 | 5.1.3.3.1 |
| Review Job Descriptions for Cyber Responsibilities | 5.1.3.3.1 | 5.1.3.3.1 | 5.1.3.3.1 |
| Inventory NG911 Hardware, Software, and Suppliers | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 |
| Assess sensitivity, integrity, and availability impact of NG911 Hardware, Software, and Suppliers | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 |
| Identify potential vulnerabilities of NG911 Hardware, Software, and Suppliers | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 |
| Develop and implement protective safeguards. | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 |
| Develop and implement functions to detect cybersecurity events. | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 |
| Develop a cybersecurity incident response plan. | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 |
| Develop cybersecurity incident recovery strategies. | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 |
| **Operations Planning** | | | |
| Interconnection Planning Procedures |  | [5.1.1](#_Interconnection) | [5.1.1](#_Interconnection) |
| Devlop Implementation Plan |  | 5.1.6.1 | 5.1.6.1 |
| Interconnection Monitoring Procedures |  | [5.1.1](#_Interconnection) | [5.1.1](#_Interconnection) |
| Staffing |  | 5.1.6.1 | 5.1.6.1 |
| Training |  | 5.1.6.1 | 5.1.6.1 |
|  |  |  |  |
| **Optional Interfaces** | | | |
| Additional Data Repository |  |  | Optional |

The following table provides a checklist to support the transition to support NG9-1-1 for Interconnected VoIP carriers. The Table cells indicates the section within the Report that provides relevant information.

Table 5 Interconnected VoIP Carrier Checklist

| **Small Carrier Checklist – Interconnected VoIP Carrier** | | | |
| --- | --- | --- | --- |
| **Essential Elements of Readiness** | **OSP Stages of Readiness** | | |
| **Legacy** | **Transitional** | **Legacy** |
| **Public Safety Governance and Regulatory Matters** | | | |
| Interaction with serving 9-1-1 Authorities, and address regulatory matters as necessary |  | 5.1.4 | 5.1.4 |
| Transition strategies |  | [5.1.4](#_Potential_State_and/or) | [5.1.4](#_Potential_State_and/or) |
| Funding |  | 5.1.5 | 5.1.5 |
| If TDM, verify whether the 9-1-1 Authority is planning to have the small carrier remain connected to the legacy selective router initially, and for how long. | [5.1.1.2](#_Originating_Service_Provider) |  |  |
| If TDM, verify the deployment of necessary LNGs (where are the LNGs proposed to be located, and where are the associated interconnection points) |  | [5.1.1.2.2](#_Transitional_Interconnection_to) |  |
| If IP-to-IP, determine if there is an IP-to-IP interconnection specifications document available and confirm the proposed points of IP-to-IP Interconnection. |  | [5.1.1.2.1](#_IP_Interconnection_to) | [5.1.1.2.1](#_IP_Interconnection_to) |
| Determine if the current 9-1-1 data process is initially expected to change, and confirm the timing of that process. |  | [5.1.1.2.1](#_IP_Interconnection_to) |  |
| Confirm the timing of transition to full i3 NG9‑1-1. |  |  | [5.1.1.2.1](#_IP_Interconnection_to) |
| In that context, compare the timing of the 9-1-1 Authority’s transition timeline in comparison to the carrier’s transition timeline towards IP transition, and reconcile any impact disparities that may generate. |  |  | [5.1.1.2.1](#_IP_Interconnection_to) |
|  |  |  |  |
| **Routing & Location** | | | |
| pANI Routing | 5.1.1.1.3 | 5.1.1.1.3 |  |
| GIS Routing |  |  | 5.1.2 |
| Location in INVITE (LbyV) |  |  | 5.1.1.2.1 |
| Access to Forest Guide |  |  | 5.2.2 |
|  |  |  |  |
| **GIS Data** | | | |
| Access to GIS for validation |  |  | 5.1.2.1 |
| Access to GIS for routing |  |  | 5.1.2.1 |
|  |  |  |  |
| **Network** | | | |
| Interconnection Agreements | 5.1.1.1.3 | 5.1.1.1.3 | 5.1.1.2.1.1 |
| IP-based Network with TDM Gateway | 5.1.1.1.3 | 5.1.1.1.3 |  |
| IP-based Core Network |  |  | 5.1.1.2.1 |
| LNG |  | 5.1.1.2.2.1  5.1.1.2.2.2  5.1.1.2.2.3 |  |
| Location Validation (LVF) |  |  | 5.1.2.1 |
| LIS |  |  | 5.1.2.1 |
| **Security** | | | |
| Establish Cyber Team | 5.1.3.3.1 | 5.1.3.3.1 | 5.1.3.3.1 |
| Clarify Roles of Cyber Team | 5.1.3.3.1 | 5.1.3.3.1 | 5.1.3.3.1 |
| Identify Cyber Education and Training | 5.1.3.3.1 | 5.1.3.3.1 | 5.1.3.3.1 |
| Review Job Descriptions for Cyber Responsibilities | 5.1.3.3.1 | 5.1.3.3.1 | 5.1.3.3.1 |
| Inventory NG911 Hardware, Software, and Suppliers | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 |
| Assess sensitivity, integrity, and availability impact of NG911 Hardware, Software, and Suppliers | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 |
| Identify potential vulnerabilities of NG911 Hardware, Software, and Suppliers | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 |
| Develop and implement protective safeguards. | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 |
| Develop and implement functions to detect cybersecurity events. | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 |
| Develop a cybersecurity incident response plan. | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 |
| Develop cybersecurity incident recovery strategies. | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 |
| **Operations Planning** | | | |
| Interconnection Planning Procedures |  | [5.1.1](#_Interconnection) | [5.1.1](#_Interconnection) |
| Devlop Implementation Plan |  | 5.1.6.1 | 5.1.6.1 |
| Interconnection Monitoring Procedures |  | [5.1.1](#_Interconnection) | [5.1.1](#_Interconnection) |
| Staffing |  | 5.1.6.1 | 5.1.6.1 |
| Training |  | 5.1.6.1 | 5.1.6.1 |
|  |  |  |  |
| **Optional Interfaces** | | | |
| Additional Data Repository |  |  | Optional |

The following table provides a checklist to support the transition to support NG9-1-1 for small cable carriers (e.g. regional cable providers). The Table cells indicates the section within the Report that provides relevant information.

Table 6 Small Cable Carrier Checklist

| **Small Carrier Checklist – Cable Carrier** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Essential Elements of Readiness** | | **OSP Stages of Readiness** | | | |
| **Legacy** | **Transitional** | **Legacy** | |
| **Public Safety Governance and Regulatory Matters** | | | | | |
| Interaction with serving 9-1-1 Authorities, and address regulatory matters as necessary | |  | 5.1.4 | 5.1.4 | |
| Transition strategies | |  | [5.1.4](#_Potential_State_and/or) | [5.1.4](#_Potential_State_and/or) | |
| Funding | |  | 5.1.5 | 5.1.5 | |
| If TDM, verify whether the 9-1-1 Authority is planning to have the small carrier remain connected to the legacy selective router initially, and for how long. | [5.1.1.2](#_Originating_Service_Provider) |  |  |
| If TDM, verify the deployment of necessary LNGs (where are the LNGs proposed to be located, and where are the associated interconnection points) |  | [5.1.1.2.2](#_Transitional_Interconnection_to) |  |
| If IP-to-IP, determine if there is an IP-to-IP interconnection specifications document available and confirm the proposed points of IP-to-IP Interconnection. |  | [5.1.1.2.1](#_IP_Interconnection_to) | [5.1.1.2.1](#_IP_Interconnection_to) |
| Determine if the current 9-1-1 data process is initially expected to change, and confirm the timing of that process. |  | [5.1.1.2.1](#_IP_Interconnection_to) |  |
| Confirm the timing of transition to full i3 NG9‑1-1. |  |  | [5.1.1.2.1](#_IP_Interconnection_to) |
| In that context, compare the timing of the 9-1-1 Authority’s transition timeline in comparison to the carrier’s transition timeline towards IP transition, and reconcile any impact disparities that may generate. |  |  | [5.1.1.2.1](#_IP_Interconnection_to) |
|  |  |  |  |
| **Routing & Location** | | | | | |
| pANI Routing | | 5.1.1.1.4 | 5.1.1.1.4 |  | |
| GIS Routing | |  |  | 5.1.2 | |
| Location in INVITE (LbyV) | |  |  | 5.1.1.2.1 | |
| Access to Forest Guide | |  |  | 5.2.2 | |
|  | |  |  |  | |
| **GIS Data** | | | | | |
| Access to GIS for validation | |  |  | 5.1.2.1 | |
| Access to GIS for routing | |  |  | 5.1.2.1 | |
|  | |  |  |  | |
| **Network** | | | | | |
| Interconnection Agreements | | 5.1.1.1.4 | 5.1.1.1.4 | 5.1.1.2.1.1 | |
| IP-based Network with TDM Gateway | | 5.1.1.1.4 | 5.1.1.1.4 |  | |
| IP-based Core Network | |  |  | 5.1.1.2.1 | |
| LNG | |  | 5.1.1.2.2.1  5.1.1.2.2.2  5.1.1.2.2.3 |  | |
| **Security** | | | | | |
| Establish Cyber Team | | 5.1.3.3.1 | 5.1.3.3.1 | 5.1.3.3.1 | |
| Clarify Roles of Cyber Team | | 5.1.3.3.1 | 5.1.3.3.1 | 5.1.3.3.1 | |
| Identify Cyber Education and Training | | 5.1.3.3.1 | 5.1.3.3.1 | 5.1.3.3.1 | |
| Review Job Descriptions for Cyber Responsibilities | | 5.1.3.3.1 | 5.1.3.3.1 | 5.1.3.3.1 | |
| Inventory NG911 Hardware, Software, and Suppliers | | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 | |
| Assess sensitivity, integrity, and availability impact of NG911 Hardware, Software, and Suppliers | | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 | |
| Identify potential vulnerabilities of NG911 Hardware, Software, and Suppliers | | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 | |
| Develop and implement protective safeguards. | | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 | |
| Develop and implement functions to detect cybersecurity events. | | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 | |
| Develop a cybersecurity incident response plan. | | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 | |
| Develop cybersecurity incident recovery strategies. | | 5.1.3.3.3 | 5.1.3.3.3 | 5.1.3.3.3 | |
| **Operations Planning** | | | | | |
| Interconnection Planning Procedures | |  | [5.1.1](#_Interconnection) | [5.1.1](#_Interconnection) | |
| Devlop Implementation Plan |  | 5.1.6.1 | 5.1.6.1 |
| Interconnection Monitoring Procedures | |  | [5.1.1](#_Interconnection) | [5.1.1](#_Interconnection) | |
| Staffing | |  | 5.1.6.1 | 5.1.6.1 | |
| Training | |  | 5.1.6.1 | 5.1.6.1 | |
|  | |  |  |  | |
| **Optional Interfaces** | | | | | |
| Additional Data Repository | |  |  | Optional | |

# Conclusions

As the National Emergency Number Association (NENA) observed,

*The evolution of emergency calling beyond the traditional voice 9‐1‐1 call has caused the recognition that our current E9‐1‐1 system is no longer able to support the needs of the future.   Next Generation 9‐1‐1 (NG9‐1‐1) networks replace the existing narrowband, circuit switched 9‐1‐1 networks which carry only voice and very limited data.[[43]](#footnote-43)*

Originating service providers play a key role in emergency communications. As telecommunications service providers, they are responsible for delivering emergency calls to 9‑1-1 systems in accordance with nationally adopted standards. Such standards address both how and where the call is delivered – matters of call structure and interconnection. Meeting these call delivery standards may create challenges for small originating service providers struggling to upgrade their own services. In accordance with the Working Group’s charge described earlier in this document, this Report has focused on small carrier issues impacted by NG9‑1‑1 implementation, and how small carriers can best support migration to next generation public safety services.

Carrier interconnection to an NG Emergency Services Network depends upon the capabilities of the small carrier and considerations regarding the method of interconnection. If the small carrier has deployed an all-IP network it may interconnect with the NG Emergency Services Network via IP (i.e., using the SIP protocol). If the small carrier has not deployed an IP infrastructure then the small carrier must deliver the emergency call to a gateway that then interworks with the NG Emergency Services Network.

Small carrier transition timelines will vary by carrier depending on the resources they have available to focus on the transition and the technical hurdles they face. With that in mind, small carriers should stay abreast of the NG9‑1-1 transition impacting their service area to better understand the ecosystem, timelines, and implications for their companies. It is extremely important that small carriers work with their state and/or regional 9-1-1 Authority to coordinate their transition timelines and expectations.

It is not expected that each small carrier would be able to implement every core cybersecurity service, hire cybersecurity experts, and/or provide their own in-house version of those suggested core services. Instead, cybersecurity core services, training and capabilities will likely be a combination of the most economic, technologically sound and operationally effective technologies available.

The Commission may play a role in helping facilitate this process. They are encouraged to assist in industry awareness of the CSRIC recommendations in both Task reports. More importantly, as recommend above, the Commission could help facilitate the development of standardized interconnection demarcation points and the respective roles and responsibilities of the parties.

# Appendix – Definitions

The following definitions are based on and/or are consistent with NENA’s “Master Glossary of 9-1-1 Terminology.”[[44]](#footnote-44)

| **Term** | **Description** |
| --- | --- |
| ADR (Additional Data Repository) | A data storage facility for Additional Data. The ADR dereferences a request from the NGCS or PSAP to return additional information about the call, caller or location. |
| ALI (Automatic Location Identification) | The automatic display at the PSAP of the caller’s telephone number, the address/location of the telephone and supplementary emergency services information of the location from which a call originates. |
| ANI (Automatic Number Identification) | Telephone number associated with the access line from which a call originates. |
| ATIS (Alliance for Telecommunications Industry Solutions) | A U.S.-based organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. [www.atis.org](http://www.atis.org) |
| BGCF (Border Gateway Control Function) | In an IMS network the BGCF selects a MGCF which will be responsible for the interworking with the PSTN or legacy Emergency Network. |
| CPE (Customer Premises Equipment) | Communications or terminal equipment located in the customer’s facilities – Terminal equipment at a PSAP. |
| CSRIC (Communications Security, Reliability and Interoperability Council) | The Communications Security, Reliability and Interoperability Council's (CSRIC) mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety. |
| Caller Location | Location information, in the form of a civic address or geo-coordinates, obtained by a PSAP to support the dispatch of emergency personnel. |
| E2 (E2 Interface) | An industry standard interface (defined in J-STD-036) between a Mobile Positioning Center/Global Mobile Location Center (MPC/GMLC) and an ALI database server to retrieve the caller callback number and location. |
| CSCF (Call Session Control Function) | General term for a functional entity within a IMS core network that can act as Proxy CSCF (P-CSCF), Serving CSCF (S-CSCF), Emergency CSCF (E-CSCF), or Interrogating CSCF (I-CSCF). |
| Enhanced-MF (Enhanced Multi-Frequency)  AKA: E-MF | The Enhanced MF signaling protocol, used on the E9-1-1 tandem-to-PSAP interface, is based on the Feature Group D (FG-D) protocol and supports the delivery of up to two 10-digit numbers, the first of which is preceded by two ANI information digits (i.e., ANI “II” digits). Telcordia GR-2953-CORE |
| ESRD (Emergency Services Routing Digit) | A 10-digit North American Numbering Plan number that uniquely identifies a base station, cell site, or sector that is used to route wireless emergency calls through the network. The ESRD may also be used by the PSAP to retrieve the associated ALI data. |
| ESRK Emergency Services Routing Key) | A 10-digit North American Numbering Plan number that uniquely identifies a wireless emergency call, is used to route the call through the network, and used to retrieve the associated ALI data. |
| Forest Guide | The Forest Guide keeps track of the coverage regions for all ESInets, and thus is a resource to help determine the next appropriate ESInet to route a 9-1-1 call. Forest Guides can, in principle, be operated by anybody, including voice service providers, Internet access providers, dedicated services providers, and enterprises. The authoritative owners of the GIS data are responsible to arrange for their coverage regions to be provisioned in such Forest Guides. |
| GIS (Geographic Information System) | A system for capturing, storing, displaying, analyzing and managing data and associated attributes which are spatially referenced. |
| ESZ (Emergency Service Zone) | A geographical area that represents a unique combination of emergency service agencies (e.g., Law Enforcement, Fire and Emergency Medical Service) that are within a specified 9-1-1 governing authority's jurisdiction. |
| HELD (HTTP Enabled Location Delivery) | A protocol that can be used to acquire Location Information (LI) from a LIS within an access network as defined in IETF RFC 5985. |
| HVAC (Heating, Ventilation, and Air Conditioning) | The system used to provide heating and cooling services to buildings.  Attribution: Public Domain |
| IETF (Internet Engineering Task Force) | Lead standard setting authority for Internet protocols. |
| ILEC (Incumbent Local Exchange Carrier) | A telephone company that had the initial telephone company franchise in an area. |
| IMS (Internet Protocol Multimedia Subsystem) | The IP Multimedia Subsystem comprises all 3GPP/3GPP2 core network elements providing IP multimedia services that support audio, video, text, pictures alone or in combination delivered over a packet switched domain. |
| INVITE | A SIP Method used to initiate a 2-way session which may include voice, text and video. |
| IP (Internet Protocol) | The method by which data is sent from one computer to another on the Internet or other networks. |
| LIS (Location Information Server) | A Location Information Server (LIS) is a functional element in an IP-capable originating network that provides locations of endpoints (i.e., calling device). The LIS is also the entity that provides the dereferencing service, exchanging a location reference for a location value. |
| LNG (Legacy Network Gateway) | An NG9-1-1 Functional Element that provides an interface between a non-IP originating network and a Next Generation Core Services (NGCS) enabled network. |
| LPG (Legacy PSAP Gateway) | The Legacy PSAP Gateway is a signaling and media interconnection point between an ESInet and a legacy PSAP. See the NENA Master Glossary for more details. |
| LRF (Location Retrieval Function) | The IMS associated functional entity that handles the retrieval of location information for the emergency caller including, where required, interim location information, initial location information and updated location information. The LRF may interact with a separate RDF or contain an integrated RDF in order to obtain routing information for an emergency call. |
| LS (Location Server) | The Location Server acquires the UE location if necessary. |
| LSRG (Legacy Selective Router Gateway) | The LSRG provides an interface between a 9-1-1 Selective Router and an ESInet, enabling calls to be routed and/or transferred between Legacy and NG networks. A tool for the transition process from Legacy 9-1-1 to NG9-1-1. |
| MF (Multi-Frequency) | A type of in-band signaling used on analog interoffice and 9-1-1 trunks. |
| MGCF | The Media Gateway Control Function (MGCF) interworks calls between the Common IMS network and the legacy emergency services network. |
| MLP (Mobile Location Protocol) | A protocol that may be used for mobile location queries. In some networks, especially in Canada, it is use in place of the E2 protocol. |
| MMES | Multi-Media Emergency Service |
| MPC/GMLC | The Mobile Positioning Center/Global Mobile Location Center (MPC/GMLC) is a Functional Entity that provides an interface between the wireless originating network and the Emergency Services Network to provide a caller’s call back number and location. See the NENA Master Glossary for more details. |
| MPLS (Multi-Protocol Label Switching) | A type of data-carrying technique for high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.  See the NENA Master Glossary for more details. |
| MSAG (Master Street Address Guide) | A database of street names and house number ranges within their associated communities defining Emergency Service Zones (ESZs) and their associated Emergency Service Numbers (ESNs) to enable proper routing of 9-1-1 calls. |
| NANP (North American Numbering Plan) | An integrated telephone numbering plan serving 20 North American countries that share telephone numbers in the +1 country code. www.nationalnanpa.com |
| NASNA (National Association of State 9-1-1Administrators) | An association that represents state 9-1-1 programs in the field of emergency communications. [www.nasna911.org](http://www.nasna911.org). |
| NCAS (Non Call-path Associated Signaling) | A method for delivery of wireless 9-1-1 calls in which the Mobile Directory Number (MDN) or Mobile Integrated Services Directory Number (MSISDN) and other call associated data (i.e., the ESRD) are passed from the Mobile Switching Center through the legacy Emergency Service Network to the PSAP. |
| NENA (National Emergency Number Association) | NENA serves the public safety community as the only professional organization solely focused on 9-1-1 policy, technology, operations, and education issues. With more than 12,000 members in 48 chapters across North America and around the globe, NENA promotes the implementation and awareness of 9-1-1 and international three-digit emergency communications systems. See <http://www.nena.org/page/aboutfaq2017> for more details. |
| NG (Next Generation) | As used herein, NG refers to NG9-1-1 (Next Generation 9-1-1)  NG9-1-1 is an Internet Protocol (IP)-based system comprised of managed Emergency Services IP networks (ESInets), functional elements (applications), and databases that replicate traditional E9-1-1 features and functions and provides additional capabilities.  See the NENA Master Glossary for more details. |
| NPD (Numbering Plan Digit) | A component of the traditional 8-digit 9-1-1 signaling protocol between the Enhanced 9-1-1 Control Office and the PSAP CPE. Identifies 1 of 4 possible area codes. Used herein as NPD/NPA. |
| NPA (Numbering Plan Area | An established three-digit area code for a particular calling area where the first position is any number 2 through 9 and the last two (2) positions are 0 through 9. Used herein as NPD/NPA. |
| OSP (Originating Service Provider) | Specifically, in this Report, an OSP routes the 9-1-1 calls placed by its customers to the appropriate Emergency Services Network. |
| Phase I | The delivery of a wireless 9-1-1 call with callback number and identification of the cell-tower from which the call originated. Call routing is usually determined by cell-sector. Required by FCC Report and Order 96-264 pursuant to Notice of Proposed Rulemaking (NPRM) 94-102. |
| Phase II | Required by FCC Report and Order 96-264 pursuant to Notice of Proposed Rulemaking (NPRM) 94-102. The delivery of a wireless 9-1-1 which is routed in the same manner as a Phase I call, but also delivers the Phase II location of the caller as defined within the FCC rules. |
| POI (Point of Interconnection) | The Point of Interconnection is a physical demarcation between an originating carrier network and an E9-1-1 or NG9-1-1 network. |
| PSAP (Public Safety Answering Point) | An entity responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy.  See the NENA Master Glossary for more details. |
| PSTN (Public Switched Telephone Network) | The network of equipment, lines, and controls assembled to establish communication paths between calling and called parties in North America |
| RDF (Routing Determination Function) | The IMS-associated functional entity, which may be integrated in an LRF, or separate to it, and provides the proper routing address that the LRF returns to the E-CSCF for routing the emergency request towards a PSAP. |
| Routing Location | Location information, in the form of a civic address or geo-coordinates, is used by routing elements in the NG9-1-1 architecture to route an emergency call.  See the NENA Master Glossary for more details. |
| SIP (Session Initiation Protocol) | A protocol specified by the IETF (RFC3261) that defines a method for establishing multimedia sessions. Used as the call signaling protocol in VoIP, NENA i2, NENA i3 and IMS. |
| SR (Selective Router) | The Central Office element (sometimes called a 9-1-1 tandem switch) that provides the switching of 9-1-1 calls. It controls delivery of the voice call with ANI to the PSAP and provides Selective Routing, Speed Calling, Selective Transfer, Fixed Transfer, and certain maintenance functions for each PSAP. |
| SRDB (Selective Routing Database) | The routing table that contains telephone number to ESN relationships which determines the routing of E9-1-1 calls. |
| SSP (System Service Provider) | As used herein, SSP refers to an Emergency System Service Provider which may be a NG9-1-1 SSP or E9-1-1 SSP. An SSP is the entity/stakeholder that provides systems and support necessary to enable 9-1-1 calling to one or more Public Safety Answering Points (PSAPs) in a specific geographic area. For E9-1-1 it is typically, but not always, an Incumbent Local Exchange Carrier (ILEC). Based on NENA’s Master Glossary, with some modifications for contextual accuracy herein. |
| TFOPA (Task Force on Optimal Public Safety Answering Point Architecture) | The FCC's Task Force on Optimal Public Safety Answering Point (PSAP) Architecture (Task Force or TFOPA) was directed to study and report findings and recommendations on structure and architecture in order to determine whether additional consolidation of PSAP infrastructure and architecture improvements would promote greater efficiency of operations, safety of life, and cost containment, while retaining needed integration with local first responder dispatch and support |
| UE (User Equipment) | A device allowing a user access to network services. |
| URI (Uniform Resource Identifier) | A URI is an identifier consisting of a sequence of characters matching the syntax rule that is named <URI> in RFC 3986. It enables uniform identification of resources via a set of naming schemes. See the NENA Master Glossary for more details. |
| URN (Uniform Resource Number Name) | A URN is a type of URI. Uniform Resource Names (URNs) are intended to serve as persistent, location-independent, resource identifiers and are designed to make it easy to map other namespaces (which share the properties of URNs) into URN-space. An example of a URN is urn:service.sos. RFC 2141 |
| VPN (Virtual Private Network) | A network implemented on top of another network (e.g. the Internet), and private from it, providing transparent services between networks or devices and networks. VPNs often use some form of cryptographic security to provide this separation. |
| WAN (Wide Area Network) | A wide area network (WAN) is a computer network that spans a relatively large geographical area and consists of two or more interconnected local area networks (LANs). |
| WCM (Wireline Compatibility Mode) | Wireline Compatibility Mode is a Wireless Phase II method in which the ESRK is delivered to the PSAP and the PSAP uses that ESRK to query for the caller’s location and call back number. |

1. See: Revision of the Commission’s Rules To Ensure Compatibility with Enhanced 911 Emergency Calling Systems; Request of King County, Washington, CC Docket No. 94-102, Order on Reconsideration, 17 FCC Rcd 14789, ¶ 1 (2002) (“King County Decision”) ( available at <https://transition.fcc.gov/Bureaus/Wireless/Orders/2001/kingco.pdf>). [↑](#footnote-ref-1)
2. See: <http://www.ng911now.org/about-ng911> [↑](#footnote-ref-2)
3. FCC TFOPA Working Group 2 Phase II Supplemental Report: NG9-1-1 Readiness Scorecard, December 2, 2016. See: [https://transition.fcc.gov/pshs/9-1-1/TFOPA/TFOPA\_WG2\_Supplemental\_Report-120216.pdf](https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG2_Supplemental_Report-120216.pdf) [↑](#footnote-ref-3)
4. See Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 9-1-1 Emergency Calling Systems; Phase II Compliance Deadlines for Non-Nationwide Carriers, Order to Stay, 17 FCC Rcd 14841, 14846-48 paras. 19-24 (2002) (Order to Stay). <https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-123A1.pdf> [↑](#footnote-ref-4)
5. FCC, In the Matter of Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993 Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services, WT Docket No. 17-69, September 27, 2017, ¶8. [↑](#footnote-ref-5)
6. The Competitive Carriers Association (CCA) represents member CMRS providers with licenses providing “two-way” wireless communications service and, together with all its affiliates, not have more than 80 million subscribers at the time original application is submitted. See: <https://ccamobile.org/> On the other hand, the Rural Wireless Association (RWA) The Rural Wireless Association represents carrier members with fewer than 100,000 subscribers. See: <http://ruralwireless.org/about-rwa/> [↑](#footnote-ref-6)
7. In addition, *47 USC 251* deals with the general duty of Telecommunications to interconnect. Under that, Section (f) addresses “Exemptions, Suspensions, and Modifications,” including “Certain Rural Telephone Companies,” and the nature of those exemptions and modifications that apply to Rural Telephone Companies. [↑](#footnote-ref-7)
8. Neither the Commission nor the Small Business Administration (SBA) has developed a small business size standard specifically for providers of incumbent local exchange services. The closest applicable size standard under SBA rules is for “Wired Telecommunications Carriers.” Under that definition, a carrier is small if it has 1,500 or fewer employees. According to the FCC’s Telephone Trends Report data, 1,307 incumbent LECs reported that they were engaged in the provision of local exchange services. Of these 1,307 carriers, an estimated 1,006 have 1,500 or fewer employees and 301 have more than 1,500 employees. [↑](#footnote-ref-8)
9. The American Cable Association (ACA) represents small and medium-sized cable operators before the U.S. Congress, Federal Communications Commission and other federal agencies. See: <http://www.americancable.org/> [↑](#footnote-ref-9)
10. In the Matter of Small Business Exemption From Open Internet Enhanced Transparency Requirements, GN Docket No. 14-28, March 2, 2017. See: <https://www.fcc.gov/document/small-business-exemption-order> [↑](#footnote-ref-10)
11. [https://c.ymcdn.com/sites/www.nena.org/resource/resmgr/ng9-1-1\_project/whatisng9-1-1.pdf](https://c.ymcdn.com/sites/www.nena.org/resource/resmgr/ng9-1-1_project/whatisng911.pdf) [↑](#footnote-ref-11)
12. The NG9-1-1 Now Coalition is comprised of leading 9-1-1 associations in the country, i.e., the National Emergency Number Association (NENA), the National Association of State 9-1-1 Administrators (NASNA), and the Industry Council for Emergency Response Technologies (iCERT), and is working in cooperation with the NG9-1-1 Institute and experts in government and academia. The Coalition is focused on rapidly accelerating the deployment of NG9-1-1. See: [http://www.ng9-1-1now.org/index#about](http://www.ng911now.org/index#about) [↑](#footnote-ref-12)
13. For example, see: Telsis, “Service Considerations during TDM to IP Migration,” <https://www.telsis.com/service-considerations-during-tdm-to-ip-migration/> As they indicate, “[f]rom reading the latest headlines in the media, you would think that the only things telcos care about right now are 5G, NFV/SDN and IoT devices. While this may be valid for the upper echelons of mobile and fixed network operators, it is not the case for many telcos. Indeed, a large number of them are still sweating their legacy TDM-based assets as they look at ways to provide services to their customers that will allow them to migrate to a next-generation IP network.” [↑](#footnote-ref-13)
14. In the Matter of Implementation of the Local Competition Provisions in the Telecommunications Act of 1996, CC Docket Nos. 96-98 and 95-185 (rel. Aug. 8, 1996) (available at <https://transition.fcc.gov/Bureaus/Common_Carrier/Orders/1996/fcc96325.pdf>). [↑](#footnote-ref-14)
15. Cf., CenturyLink | Wholesale | Access to Emergency Services (9-1-1 - E9-1-1); Pricing, Rate Structure, (“You must provide a facility between your end-office and the designated 9-1-1 SR with the exception of Colorado where CenturyLink must come to your end-office.”) (available at http://www.centurylink.com/wholesale/pcat/911.html) [↑](#footnote-ref-15)
16. Cf., In the Matter of Nationwide Number Portability and Numbering Policies for Modern Communications, WC Docket Nos. 17-244 and 13-97, at ¶45, “Local systems, including Local Service Management Systems (LSMS) and Service Order Administration (SOA), will also be affected by a national LRN system… Current systems may rely in part upon an assumed structure whereby numbers are only ported within LATAs or NPAC regions … (footnote omitted) (available at <https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-133A1.pdf>). [↑](#footnote-ref-16)
17. Cf., Texas PUC Subst. R. 26.433 (“The MSAG must be made available to the CTU at no charge and must be in a mechanized format that is compatible with the CTU’s systems.”; “The 9-1-1 database management services provider shall make all updates to the MSAG electronically available to CTUs within 24 hours of update by the 9-1-1 administrative entity.”) (available at <http://www.puc.texas.gov/agency/rulesnlaws/subrules/telecom/26.433/26.433.pdf>). [↑](#footnote-ref-17)
18. Cf., Texas PUC Subst. R. 26.435 (“The 9-1-1 network services provider shall bill the appropriate 9-1-1 administrative entity and shall not bill a CTU for ANI, ALI, and/or selective routing services. Billing for additional or other 9-1-1 related services specifically required by a CTU is permitted.”) (available at <http://www.puc.texas.gov/agency/rulesnlaws/subrules/telecom/26.435/26.435.pdf>) [↑](#footnote-ref-18)
19. Cf., CenturyLink | Wholesale | Access to Emergency Services (9-1-1 - E9-1-1); Pricing, Rate Structure, (“The management of the E9-1-1 database is performed by Intrado Inc., who may assess charges to both CenturyLink and you for updates to the E9-1-1 database and for other services, such as providing copies of the Master Street Address Guide (MSAG). … subsequent versions on a quarterly basis at no charge. MSAGs requested outside the quarterly schedule will be provided and you will be charged on an Individual Case Basis (ICB).”) (Emphasis Added) (available at http://www.centurylink.com/wholesale/pcat/911.html) [↑](#footnote-ref-19)
20. Note that the media interconnection, not shown, is also at the BCF. [↑](#footnote-ref-20)
21. LIS or equivalent elements may be operated directly by originating service providers, by their chosen vendors, or possibly by a 9-1-1 Authority, a set of 9-1-1 Authorities, or their vendors as a service to carriers – this may vary across a variety of NG9-1-1 service systems throughout the USA and North America. [↑](#footnote-ref-21)
22. Some would view that the GIS data is part of and internal to the NG9-1-1 system, others will view that it is external and utilized via the Spatial Interface for functions that are internal to the NG9-1-1 Core Services architecture. [↑](#footnote-ref-22)
23. “National Initiative for Cybersecurity Education (NICE),” <https://www.nist.gov/itl/applied-cybersecurity/nice>, accessed on March 4, 2018. [↑](#footnote-ref-23)
24. “NICE Framework Specialty Areas and Work Role Table of Contents,” <<https://www.nist.gov/file/372581>>, accessed on March 4, 2018. [↑](#footnote-ref-24)
25. “DRAFT National Cybersecurity Workforce Framework,” <https://www.nist.gov/file/359261>, accessed on March 4, 2018. [↑](#footnote-ref-25)
26. “Emergency Services Sector Cyber Risk Assessment,” <https://www.dhs.gov/sites/default/files/publications/Emergency-Services-Sector-Cyber-Risk-Assessment-508.pdf>, accessed on March 4, 2018. [↑](#footnote-ref-26)
27. “Emergency Services Sector Roadmap to Secure Voice and Data Systems,” <https://www.dhs.gov/sites/default/files/publications/Emergency-Services-Sector-Roadmap-to-Secure-Voice-and-Data%20Systems-508.pdf>, accessed on March 4, 2018. [↑](#footnote-ref-27)
28. “National Cyber Awareness System,” <https://www.us-cert.gov/ncas>, accessed on March 4, 2018. [↑](#footnote-ref-28)
29. “Information Sharing Specifications for Cybersecurity,” <https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity>, accessed on March 4, 2018. [↑](#footnote-ref-29)
30. “Stop.Think.Connect.” <https://www.dhs.gov/stopthinkconnect>, accessed on March 4, 2018. [↑](#footnote-ref-30)
31. In the Matter of Implementation of the Local Competition Provisions in the Telecommunications Act of 1996, CC Docket Nos. 96-98 and 95-185 (rel. Aug. 8, 1996) (available at <https://transition.fcc.gov/Bureaus/Common_Carrier/Orders/1996/fcc96325.pdf>). [↑](#footnote-ref-31)
32. “Ninth Annual Report to Congress on State Collection and Distribution of 9-1-1 and Enhanced 9-1-1 Fees and Charges,” <[https://www.fcc.gov/files/9thannual9-1-1feereportpdf](https://www.fcc.gov/files/9thannual911feereportpdf)>, accessed on April 10, 2018. [↑](#footnote-ref-32)
33. Wireless Infrastructure Association, Rural America: How Wireless Technologies Could Impact America’s Heartland, June 12, 2017, p 7. See: <http://www.networkbuilding.com/wp-content/uploads/WIA_RuralAmerica-2-PRINT1.pdf> [↑](#footnote-ref-33)
34. Ibid. [↑](#footnote-ref-34)
35. “Statement of Chairman Ajit Pai on Projected USF Budget Cuts for Small, Rural Carriers,” May 1, 2018. See: <https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0501/DOC-350513A1.pdf> See also: FCC Notice of Proposed Rulemaking (NPRM), In the Matter of Connect America Fund, ETC Annual Reports and Certifications, Establishing Just and Reasonable Rates for Local Exchange Carriers, Developing a Unified Intercarrier Compensation Regime, WC Dockets No. 10-90, No. 14-58, No. 07-135, No. 01-92 (Adopted: March 14, 2018, Released: March 23, 2018). <https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0426/FCC-18-29A1.pdf> As noted in the introduction to the proceeding: “Universal service can—and must—play a critical role in helping to bridge the digital divide to ensure that rural America is not left behind as broadband services are deployed. The directive articulated by the Commission in 2011 remains as true today as it did then: “The universal service challenge of our time is to ensure that all Americans are served by networks that support high-speed Internet access.” Though we have made progress for rural Americans living in areas served by our nation’s largest telecommunications companies, the rules governing smaller, community-based providers—rate-of-return carriers—appear to make it more difficult for these providers to serve rural America. As a result, approximately 11 percent of the housing units in areas served by rate-of-return carriers lack access to 10 Mbps downstream/1 Mbps upstream (10/1 Mbps) terrestrial fixed broadband service while 34 percent lack access to 25 Mbps downstream/3 Mbps upstream (25/3 Mbps). It is time close this gap and ensure that all of those living in rural America have the high-speed broadband they need to participate fully in the digital economy.” ¶ 1. [↑](#footnote-ref-35)
36. “Potential Points of Demarcation in NG9-1-1 Networks Information Document,” NENA, pp. 9-10. See: <https://cdn.ymaws.com/www.nena.org/resource/collection/2851C951-69FF-40F0-A6B8-36A714CB085D/NENA-INF-003_Potential_Points_of_Demarcation_in_NG9-1-1_Networks.pdf?hhSearchTerms=%22NG9-1-1%22> [↑](#footnote-ref-36)
37. Ibid. As stated, *“[t]he decision we reach here addresses the issue of where the responsibilities lie between the wireless carrier and the PSAP in terms of the costs of implementing E911 Phase I service, under the facts and circumstances of this case and the record before us. We do not address the issue of which party – PSAP or carrier – may choose the transmission method and technology to be used to provide Phase I. … [W]e expect carriers to negotiate in good faith with the PSAPs concerning the appropriate Phase I technology, based on the totality of the circumstances before them, including what best serves the PSAP and their own subscribers’ interest in having timely access to E911 services.”* [↑](#footnote-ref-37)
38. See: <http://www.nasna911.org/state-911-contacts> [↑](#footnote-ref-38)
39. On September 10, 2018, the Commission released a public notice seeking comment on the vertical accuracy (z-axis) test bed report, submitted by CTIA on behalf of the nationwide wireless carriers (AT&T Mobility, Sprint, T-Mobile USA, and Verizon), and on the Carriers’ proposal for a z-axis accuracy metric submitted with the Report. As stated, “the Carriers submitted the Report and their z-axis proposal to the Commission on August 3, 2018, pursuant to the Commission’s 2015 Wireless E911 Location Accuracy Fourth Report & Order, which required the Carriers to establish a test bed process to develop a proposed z-axis accuracy metric and to submit the proposed metric to the Commission for approval.” See: <https://ecfsapi.fcc.gov/file/0910993124543/DA-18-928A1.pdf> [↑](#footnote-ref-39)
40. Ibid. Pg 11. [↑](#footnote-ref-40)
41. Ibid. Pg 13. [↑](#footnote-ref-41)
42. After the transition to support NG9-1-1, depending upon the coverage area of the small carrier, there may be a need to send 9-1-1 calls to different ESInets based upon the location of the caller. The standard method to do that in NG9-1-1 is by interrogating a “Forest Guide” with the location of the caller. The Forest Guide returns routing information (e.g. a URI) that will allow the 9-1-1 call to be sent to the appropriate ESInet.

    The Forest Guide keeps track of the coverage regions for all ESInets. Forest Guides can, in principle, be operated by anybody, including voice service providers, Internet access providers, dedicated services providers, and enterprises. The authoritative owners of the GIS data are responsible to arrange for their coverage regions to be provisioned in the Forest Guides. As of the publication of this Report the operator of the Forest Guide(s) has not been identified. [↑](#footnote-ref-42)
43. Ibid [↑](#footnote-ref-43)
44. “NENA Master Glossary of 9-1-1 Terminology,” National Emergency Number Association (NENA), revised April 2018. See: <https://www.nena.org/page/Glossary> [↑](#footnote-ref-44)