Final Report – Recommendations for 9-1-1 System Reliability and Resiliency during the NG9-1-1 Transition

Version 2.0 – March 8, 2019 (Addition of Best Practices)

Table of Contents

Table of Tables

Table of Figures

1 Results in Brief

1.1 Executive Summary

Since the first 9-1-1 call in 1968, the nation's 9-1-1 system continues to provide the capability for those in need of help to receive help during any life-threatening situation. Many existing 9-1-1 systems are well beyond end of life cycle replacement and are no longer supported by the manufacturers. As technology continues to advance, the legacy 9-1-1 system cannot meet the needs of today's technologies and a replacement technology is needed. The replacement technology, called Next Generation 9-1-1 (NG9-1-1), replaces the circuit switched technology of today's 9-1-1 system with secure Internet Protocol (IP) technology as part of the life cycle replacement of 9-1-1. Specifically, 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. NG9-1-1 is designed to provide access to emergency services from all connected communications sources, and provide multimedia data capabilities for Public Safety Answering Points (PSAPs) and other emergency service organizations. The considerations discussed in this Report will help those implementing NG9-1-1 make the transition while mitigating the risks associated with the transition.

In accordance with the specific Objectives of Working Group 1, outlined in *Section* 3, the Report provides an overview of the objectives, scope, methodology and background that the Communications Security, Reliability and Interoperability Council (CSRIC) VI Working Group 1, Task Group 1 have followed while developing the Report.

The Objectives and Scope of the Report include:

- Review of existing Best Practices regarding overall monitoring, reliability, notifications, and accountability in preventing 9-1-1 outages in transitional NG9-1-1 environments.
- Development of additional guidance on Best Practices regarding overall monitoring, reliability, notifications, and accountability in preventing 9-1-1 outages in transitional NG9-1-1 environments.
- Identifying risks associated with transitional 9-1-1 systems that could result in disruptions to 9-1-1 service.
- Making recommendations to protect the NG9-1-1 network, including recommendations for Best Practices and standards development.
- Study of specific actions that originating Service Providers, 9-1-1 System Service Providers and other entities in the 9-1-1 call chain should take to detect and deter outage precursors before 9-1-1 calls are delivered to the ESInet gateway.
- Recommended actions the Federal Communications Commission (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 would be on identifying tools that are already available or not burdensome to implement.

The Report content was developed based on industry subject matter experts represented on the Working Group and relies upon relative resource information provided in previous CSRIC efforts and the consideration of other industry documents related to the reliability of 9-1-1.

The Report defines NG9-1-1 roles and provides a common technical framework that defines functional elements, interfaces and points of demarcation for transitional and end-state NG9-1-1 architectures. As used in this Report, the demarcation points are at the boundaries between the Emergency Services Network and other partner networks with which they interconnect. The Working Group performed an analysis of the various architectures, by demarcation point and stakeholder[1] role, to identify potential points of failure with respect to emergency call delivery, location delivery and callback information delivery to Public Safety Answering Points (PSAPs). The Report concludes with an analysis and recommendations of Best Practices related to enhancing the transition from Legacy 9-1-1 to NG9-1-1, and also provides research findings on commercially available tools currently used by the private sector to detect and deter 9-1-1 outages.

Service Providers and other 9-1-1 stakeholders are encouraged to review in detail the analysis and findings contained throughout the Report, as well as the Recommendations in *Section* 13 (also summarized here for convenience), and the modified and new Best Practices provided in Appendix B –Recommended Changes to Existing 9-1-1 Related Best Practices

1.1.1 Understanding NG9-1-1 Architectures

- There is a need for Service Providers across all industry segments (cable, wireline, wireless, Interconnected VoIP) to be able to identify within their networks service-impacting events that impair or cause a total loss of service. Network events/anomalies potentially impact 9-1-1 call delivery throughout the country and the Working Group recommends that Service Providers ensure Product Management and Network Operations personnel have a thorough understanding of the functional elements that support the transitional and end-state NG9-1-1 architectures described in this Report in the following sections:
    - *Section* 4 describes various entities that have responsibility for managing risks and reporting outages in terms of stakeholder roles that are associated with different components of transitional and end-state NG9-1-1 architectures. These descriptions provide a basis for identifying the types of failures that may be visible to entities operating different components of the NG9-1-1 service architecture.
    - *Sections* 5 through 9 describe the various components of transitional and end-state NG9-1-1 architectures and define points of demarcation that denote the logical boundaries of responsibility between the stakeholders responsible for providing those components. These sections provide detailed overviews of

[1] For the purposes of capturing all companies and entities that are a part of the 9-1-1 call chain those entities are referred to as "stakeholders" throughout this Report and are defined in detail within Section 4.1.

the various transitional and end-state NG9-1-1 architectures to establish a framework for the analysis of potential failure points.

1.1.2 Identifying Risks with Transition to NG9-1-1

The Working Group studied specific types of failures that originating Service Providers, 9-1-1 System Service Providers and other entities in the 9-1-1 call chain can detect, with the objective of deterring outages before they impact 9-1-1 call and data delivery to PSAPs.

Section 10, Architectural Analysis, analyzes the transitional and end-state NG9-1-1 architectures, by demarcation point and stakeholder role, to identify potential points of failure from the perspective of:

- Call delivery failures,
- Location delivery failures, and
- Callback information delivery failures.

Potential failures in the delivery of other critical information to key architecture elements and PSAPs are also identified through the definition of the demarcation points and the high-level descriptions that comprise the architectural analysis.

This section emphasizes how transitional and end-state NG9-1-1 architectures, by their very nature, limit any given stakeholder's monitoring and reporting capabilities to those aspects of the architecture to which they have visibility.

It is recommended that Service Providers should ensure their Product Management and Network Operations personnel have a thorough understanding of the Architectural Analysis as described in this Report and have a working knowledge of where potential network failures can be experienced.

1.1.3 Recommended Actions to Detect and Deter Threats to 9-1-1

In a recent FCC publication, Summary of 9-1-1 Certification Data for 2017 [13], the Public Safety and Homeland Security Bureau reported on 188 covered entities filing certifications consistent with the FCC 9-1-1 certification rules. Service Providers are encouraged to review the findings of the Report which contains aggregate network data from communications Service Providers that offer 9-1-1, E9-1-1 or NG9-1-1 capabilities. The Report also provides insight into measures that are being taken by the industry to enhance the reliability of 9-1-1 networks and those recommendations are incorporated into this Report. The FCC can assist in the smooth transition from Legacy 9-1-1 to NG9-1-1 by encouraging Service Providers to review in detail the findings in the Summary of 9-1-1 Certification Data for 2017 as well as this CSRIC VI Report. Specific attention should be paid to the network risk findings in *Section* 10, Architectural Analysis.

For Service Providers and 9-1-1 stakeholders who do not have robust network monitoring systems, the Working Group also recommends reviewing *Section* 12, Analysis of Network Monitoring/Report Tools. Based on research conducted by the Working Group, this section of the Report provides 9-1-1 stakeholders with a better understanding of the various network elements that require monitoring and commercially available tools that can be obtained to manage the various and complex elements of communications networks. The FCC clarified in

its directive to determine if tools were commercially available and not burdensome to implement. The Working Group refrained from determining if the implementation of commercially available tools could be burdensome on a Service Provider. However, the Working Group strongly recommends that Service Providers consider incorporating network detection tools, as appropriate, to assist network operations in detecting or deterring threats to 9-1-1 before they reach the ESInet perimeter.

The Working Group recommends that Service Providers and other stakeholders work together to ensure that the system monitoring information that is needed to mitigate risks, monitor elements of the NG9-1-1 infrastructure and identify 9-1-1 outages is shared between providers and that the information is available to stakeholders when needed.

1.1.4 Best Practices

The Working Group was asked to review existing Best Practices and develop additional guidance regarding overall monitoring, reliability, notifications, and accountability in preventing 9-1-1 outages in transitional NG9-1-1 environments. Existing CSRIC Best Practices were evaluated for applicability to NG9-1-1, and gaps were observed. The Working Group made recommendations on how to fill these gaps by updating existing Best Practices and defining new Best Practices, primarily focused on the transition and introduction of NG9-1-1. The analysis and recommendations focused on:

- Monitoring, reliability, notifications, and accountability in preventing 9-1-1 outages in transitional NG9-1-1 environments;
- Facilitating the transition to NG9-1-1; and
- Aiding in the protection of the NG9-1-1 network, with Best Practices.

1.1.5 Cybersecurity Considerations

While cybersecurity considerations are an important part of the transition to NG9-1-1, this Report does not focus on cybersecurity. The Working Group recommends that stakeholders take deliberate steps to consider the cybersecurity implications introduced by the transition to NG9-1-1. The Working Group also recommends that a future CSRIC engage industry cybersecurity experts and NG9-1-1 experts to focus on NG9-1-1 related cybersecurity challenges and develop Best Practices as appropriate. See section 13.5 for further discussion.

2 Introduction

This final Report documents the efforts undertaken by the Communications Security, Reliability and Interoperability Council (CSRIC) VI Working Group 1, Task Group 1 that identifies the specific actions that originating Service Providers, 9-1-1 System Services Providers and other entities in the 9-1-1 call chain should take to detect and deter outage precursors before 9-1-1 calls are delivered to the ESInet gateway.

A separate Report, completed by CSRIC VI Working Group 1, Task 2, provides information on small carrier issues related to NG9-1-1 implementation, what barriers to implementation, if any, the FCC should address and a recommended “NG9-1-1 readiness checklist” for small carriers.

As states, regions, counties and operational areas make the transition to NG9-1-1 there are several elements that must be considered in order to ensure the 9-1-1 system remains reliable and resilient before, during and after the transition to NG9-1-1. The key elements that need to be considered are discussed in this Report.

The previous work that was summarized in the Task Force on Optimal Public Safety Answering Point Architecture (TFOPA) Working Group 1 Supplemental Report [5], the National Association of State 9-1-1 Administrators (NASNA) Model State 9-1-1 Plan [6], and the National Emergency Number Association's Standards and Best Practices [7] form the basis of this Report. While these previous works provide a good baseline, a comprehensive guide that can be used during the transition to NG9-1-1 was lacking. This Report helps to fill in the gaps in the information that is currently available.

NG9-1-1 provides many advantages over the existing 9-1-1 system, including:

- Overcoming technology limitations with today's 9-1-1 network;
- Faster call delivery;
- Increased routing capability;
- Increased routing redundancy;
- Increased ability to support call overflow and backup;
- Updated Geographic Information System (GIS) capabilities;
- Better representation of Wireless Location Data and Additional Data; and
- Enabling new technologies and media types.

The considerations that are discussed in this Report will help those implementing NG9-1-1 make the transition while mitigating the risks associated with the transition. The Report begins by providing an overview to the NG9-1-1 technology and identifies the demarcation points in a transitional 9-1-1 network as well as those demarcation points that will exist in an NG9-1-1 network.

Sections 4 through 9 define a common technical framework, based on the NENA i3 NG9-1-1 system architecture specified in NENA-STA-010 [18], that is used to describe a transitional 9-1-1 network. *Section* 10 of the Report provides an architectural analysis and identifies the risks associated with transitional 9-1-1 systems that could result in 9-1-1 service disruptions. *Section* 11 of the Report provides an analysis of Best Practices, and Section 12 provides an overview of existing tools that can be used to monitor, report and track 9-1-1 systems. The final *sections* 13 through 13.6 of the Report provide an overview of Recommendations and Conclusions.

2.1 CSRIC VI Structure

Communications Security, Reliability and Interoperability Council VI		
Working Group 1: Transition Path to NG9-1-1	Working Group 2: Comprehensive Re-imagining of Emergency Alerting	Working Group 3: Network Reliability and Security Risk Reduction [11]
Chair: Mary A. Boyd, West Safety Services	***Chair:*** Farrokh Khatibi, Qualcomm	***Chair*****:** Travis Russell, Oracle
FCC Liaisons: David Furth and John Healy	***FCC Liaisons***: Steven Carpenter and Austin Randazzo	***FCC Liaisons*****:** Steven McKinnon and Vern Mosley

Table 1 – CSRIC VI Structure

2.2 Working Group 1 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

Name	Company	Task Group
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

Name	Company	Task Group
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, Principal Member of Tech 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, Deputy Emergency Management Coordinator; Liaison to County Judge	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.

Name	Company	Task Group
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 Emergency Communication District Texas 9-1-1 Alliance	Task 2
Robert Sherry, Senior Systems Engineer	West Safety Services	Task 1 & 2

Table 3 - List of Subject Matter Experts

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

Name	Company	Task Group
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, FCC	Federal Communications Commission	Task 1 & 2

Table 4 - List of FCC Liaisons

3 Objective, Scope, and Methodology for Working Group 1 Task 1

3.1 Objective for Working Group 1 Task 1

The nation's transition from Legacy 9-1-1 circuit switched network call handling platforms to NG9-1-1 IP-based Emergency Services IP networks (ESInets) and core services presents the opportunity to assess the reliability and resiliency of the networks and functional elements supporting the transition. The CSRIC VI Working Group 1 has been charged with examining various element of the Legacy 9-1-1 and NG9-1-1 network and making recommendations that assist stakeholders with the transition.

Specifically, Working Group 1 was charged with the following tasks:

- Review existing Best Practices regarding overall monitoring, reliability, notifications, and accountability in preventing 9-1-1 outages in transitional NG9-1-1 environments.
- Develop additional guidance on Best Practices regarding overall monitoring, reliability, notifications, and accountability in preventing 9-1-1 outages in transitional NG9-1-1 environments.
- Identify risks associated with transitional 9-1-1 systems that could result in disruptions to 9-1-1 service.
- Make recommendations to protect the NG9-1-1 network, including recommendations for Best Practices and standards development.

- Study specific actions that originating Service Providers, 9-1-1 System Service Providers and other entities in the 9-1-1 call chain should take to detect and deter outage precursors before 9-1-1 calls are delivered to the ESInet gateway.
- 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 would be on Identifying tools that are already available or not burdensome to implement.

Working Group 1 was organized into two separate Task Groups to address the deliverables described above, referred to as Task 1: 9-1-1 System Reliability and Resiliency during the NG9-1-1 Transition, and Task 2: Small Carrier NG9-1-1 Transition Considerations.

In regard to Task-1, the FCC directed CSRIC VI 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.

In regard toTask-2, the FCC directed CSRIC VI to advise the FCC on small carrier issues related to NG9-1-1 implementation, including recommendations on how the FCC could address these issues. This included advice on what small carriers in the state or region need to do to be ready on time to deliver their 9-1-1 traffic in an NG9-1-1compatible manner; what economic disadvantages, if any, may impede small carriers in implementation of NG9-1-1; and what barriers to implementation, if any, the FCC should address. CSRIC VI was also asked to recommend a “NG9-1-1 readiness checklist” for small carriers analogous to the one the Task Force on Optimal Public Safety Answering Point Architecture (TFOPA) [3] developed for PSAPs.

This Report is dedicated to the deliverables and recommendations of Task 1. The findings and recommendations of Task 2 were drafted and adopted by CSRIC VI in a separate Report in the Fall of 2018.

3.2 Scope for Working Group 1 Task 1

As described above, the first task of the Working Group was to review existing Best Practices and develop additional guidance regarding overall monitoring, reliability, notifications, and accountability in preventing 9-1-1 outages in transitional NG9-1-1 environments. In particular, the Working Group identified risks associated with transitional 9-1-1 systems that could result in disruptions to 9-1-1 service and make recommendations to protect them, including recommendations for Best Practices and standards development.

In the first version of this Report, the Working Group performed an initial analysis of existing Best Practices. The Working Group studied specific actions that originating Service Providers, 9-1-1 System Service Providers and other entities in the 9-1-1 call chain should take to detect

and deter outage precursors before 9-1-1 calls are delivered to the ESInet gateway[2]. For the purposes of capturing all companies and entities that are a part of the 9-1-1 call chain those entities are referred to as "stakeholders" throughout this Report and are defined in detail within *Section 4.1*.

In this second version of the Task 1 Report, modifications to existing Best Practices are proposed and new Best Practices are identified.

3.3 Methodology for Working Group 1 Task 1

3.3.1 Analysis of Failure Detection Points in Transitional and End-State NG9-1-1 Architectures

Based on a review of ATIS-0500034 [1], Working Group members were able to describe transitional and end-state NG9-1-1 architectures and stakeholder roles applicable to those architectures. Having gained an understanding of the functional elements and interfaces that comprise the various architectures, the Working Group then identified points of demarcation applicable to the NG9-1-1 architectures, denoting the logical boundaries of responsibility between the stakeholders. The Working Group then performed an analysis of the various architectures, by demarcation point and stakeholder role, to identify potential points of failure with respect to emergency call delivery, location delivery and callback information delivery to Public Safety Answering Points (PSAPs). These particular failure types were selected for analysis because of their alignment with existing E9-1-1 metrics associated with call delivery and Automatic Number Identification (ANI)/Automatic Location Identification (ALI) failures. The Working Group recognized that ALI failures include a failure to deliver both location and non-location information such as Class of Service, and Service Provider contact information. In an NG9-1-1 environment, non-location ALI-type information is conveyed as "Additional Data." While the analysis did not include separate subsections associated with failures to deliver "Additional Data", the Working Group addressed Additional Data delivery through the definition of the demarcation points and the high-level descriptions provided as part of the architectural analysis.

3.3.2 Methodology of the Analysis of Best Practices

The Best Practices review process consisted of an initial review of the existing FCC Best Practices, of which there are over 1000. The Working Group assessed each Best Practice to assure it was still accurate and to determine whether it applied to Public Safety. Where applicable, "Public Safety" was added if not already included in the Best Practice. In addition, some Best Practices associated with emergency services were modified (updated) to reflect their applicability to not only E9-1-1, but NG9-1-1. As gaps were identified, the Working Group defined new Best Practices that are applicable to emergency services, specifically NG9-1-1. Also, the Working Group identified a new Keyword called "Interconnection" associated with those Best Practices that were applicable to cases where two or more parties connect their

[2] The term ESInet gateway was interpreted to mean the generic egress from an Originating Service Provider to an ESInet.

networks, or for cases of interoperability between to two or more parties. The modified Best Practices are provided in the tables in Appendix B –Recommended Changes to Existing 9-1-1 Related Best Practices

3.3.3 Methodology of Network Monitoring/ Reporting Tool Research

The methodology conducted in order to make recommendations on 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 was achieved through research with member companies of the Working Group. The focus of the research was on identifying tools that were commercially available, or if tools being used to detect and deter network anomalies were proprietary or internally developed systems. The FCC charter also clarified that the tools were not to be burdensome to implement. The Working Group believed it was not in the position to determine if its findings were burdensome on a carrier and this is discussed further in *Section* 12 of the Report.

The research sought to understand:

- What tools responding companies used to detect, deter and report transport related issues. Are those tools commercially available, or developed internally by the responding organization?
- What tools responding companies used to detect and report any routing related issues (E9-1-1 and NG9-1-1 environments)? Are those tools commercially available, or developed internally by the responding organization?
- What tools responding companies used to detect and report any proxy or other NG9-1-1 related issues which would apply if the responding organizations were running any of its own NG9-1-1 functional elements such as a Location Information Server (LIS), Legacy Network Gateway (LNG) or Legacy Selective Router Gateway (LSRG)? Are those tools commercially available, or developed internally by the responding organization?
- What tools responding companies used to detect and report any cyber or information security threat related issues? Are those tools commercially available, or developed internally by the responding organization?
- Which information security management framework(s) (if any) was applied to a responders NG9-1-1 products and services (if applicable)?
- What other recommendations, tools, key performance indicators or capabilities are available that will assist in ensuring network reliability and help increase the situational awareness capabilities of the NG9-1-1 Service Providers, 9-1-1 Administrators, and/or PSAPs?

The results of the research can be found in *Section* 12 Analysis of Network Monitoring/Reporting Tool Research.

4 Background

4.1 Definition of 9-1-1 Networks and Services

There is a need for Service Providers across all industry segments (cable, wireline, and wireless), in all stages of the Public Switched Telephone Network (PSTN) transition, to be able to identify when their networks may be experiencing service-impacting events that impair or cause the total loss of 9-1-1 services. As service architectures to support 9-1-1 calling and data delivery evolve to NG9-1-1, there is a need to better understand the complexities of how NG9-1-1 service architectures are designed and where they diverge from the pre-existing legacy E9-1-1 network infrastructures. This information will be critical for Service Providers to know so as to:

a) collect network information that may be reportable under the Part 4 Rules [14] [15];
b) define new metrics to support such reporting requirements, and
c) determine if standardization efforts are needed related to those new metrics for data collection.

The purpose of this section is to compare the service architectures used today to provide E9-1-1, with transitional and end-state NG9-1-1 service architectures and to identify where in those architectures service-impacting events can be detected. However, it should be noted that the technical limitations outlined in this Report limit any given stakeholder's monitoring and reporting capabilities; that cannot be understated.

4.1.1 Stakeholders

It is important to identify stakeholders who have responsibility for managing risks and reporting outages. The TFOPA report [4] defines stakeholders and ATIS-0500034 [1] expands these to provide more granularity when assessing where failures may occur and how remedies may be applied.

4.1.1.1 TFOPA Description of Stakeholder Roles

The TFOPA report defines three stakeholders as shown in Figure 1. It defines the Originating Service Environment (OSE), 9-1-1 System Service Provider, and Local 9-1-1 Authority (including the PSAP).

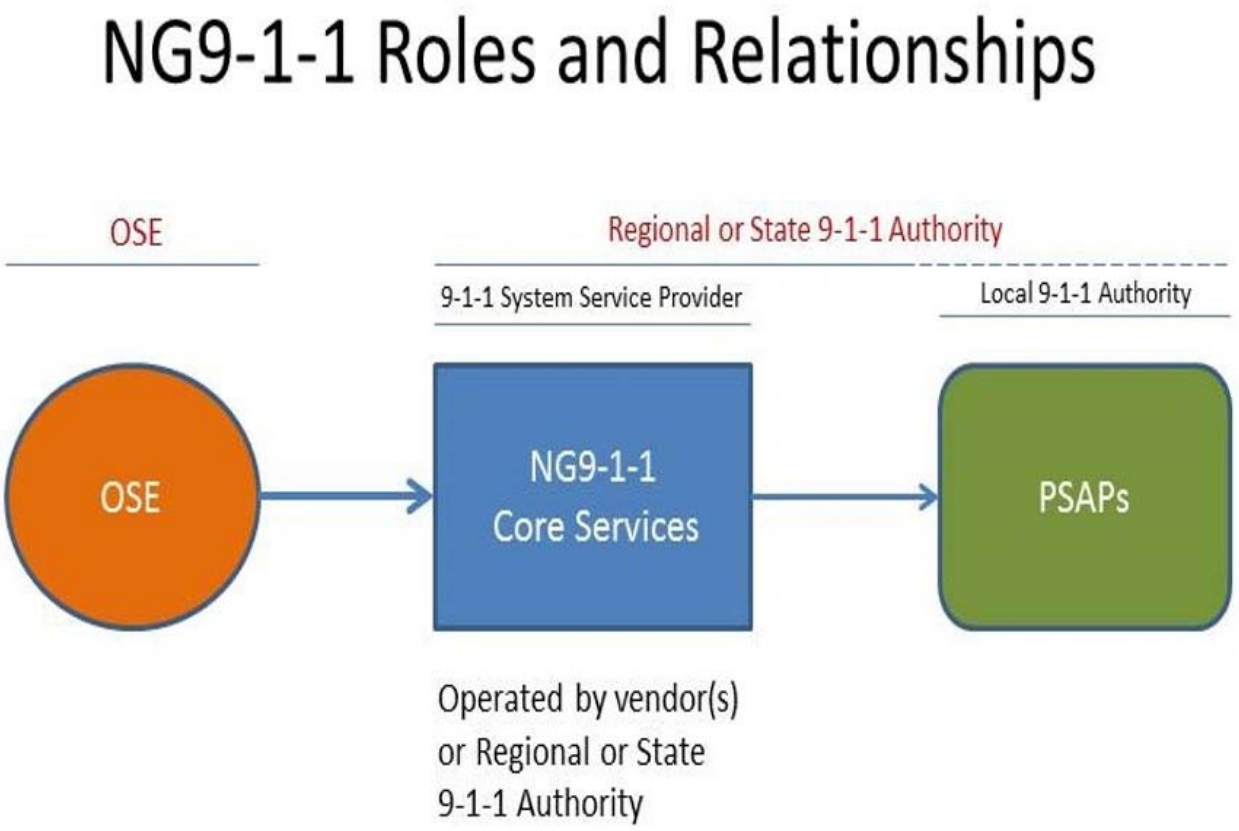


Figure 1 – TFOPA Roles and Relationships

The TFOPA report defines originating Service Provider stakeholders as:

"This report introduces the expanded nature of NG9-1-1, including what is termed the Originating Service Environment (OSE). This environment includes IP call set-up, location determination, validation and delivery to ESInets across the country."

The TFOPA report defines 9-1-1 System Service Provider as:

***"9-1-1 System Service Provider:** the operational and management entity that provides and runs the central 9-1-1 core services components."*

The TFOPA report defines 9-1-1 Authorities as:

"There are many variations on roles between 9-1-1 Authorities at local, regional, and state levels (including some areas where none of the three formally exist). When viewed at a national level however, there is a gradual trend toward the roles and relationships depicted above as NG9-1-1 work proceeds. The 9-1-1 Authority term is somewhat generic, as the name of organizations that fill that role vary greatly, such as 9-1-1 Administrator, Emergency Telephone Service Board (ETSB), etc. In many cases, the regional or state 9-1-1 Authority does not have direct governance over the local 9-1-1 Authorities. As this report discusses, referencing the organizational roles in the figure above instead of just the physical components involved is one way to more clearly state the nature of relationships in the 9-1-1 environment."

ATIS-0500034 [1] discusses stakeholders in similar categories but provides more granularity in order to enumerate the methods for reporting, monitoring and risk management.

4.1.1.2 Description of Stakeholder Roles in ATIS-0500034

Stakeholder Role descriptions provide a common understanding of how the terms are used within ATIS-0500034 [1]. The rationale is that not everyone will know what any of these roles do and do not do. These Stakeholder Roles may be implementation and business model specific.

It is also important to point out that sometimes any single company/entity might serve in multiple roles, e.g., an Incumbent Local Exchange Carrier (ILEC) could be serving as an Originating Service Provider (OSP) (legacy or IP-based), a Legacy Network Gateway (LNG) operator, an NG9-1-1 System Service Provider (NG9-1-1SSP), a Legacy PSAP Gateway (LPG) Operator, and Location Retrieval Function (LRF) Operator, or any combination of those. A government entity (e.g., 9-1-1 Authority) could serve in any of these roles. And in some cases, the provider of any of these roles may not be subject to FCC reporting responsibilities.

To the extent possible, the following descriptions are based on the National Emergency Number Association (NENA) Master Glossary of 9-1-1 Terminology [8].

4.1.1.2.1 Originating Service Provider (OSP) Using Legacy Technology[3]

A legacy-based OSP role provides the ability for a caller to make calls. In the context of this document, it is focused on the ability to make 9-1-1 calls. It is the OSP's responsibility to forward 9-1-1 calls toward the serving Emergency Services Network. Since the legacy-based OSP is using non-IP technology, calls destined for an NG Emergency Services Network must go through a gateway.

The OSP-Legacy role may be provided by traditional "phone companies", competitive "phone companies", or other private or public communications entities that are not using IP-based technology.

4.1.1.2.2 Originating Service Provider (OSP)-IP-Based Technology

An IP-based OSP role provides the ability for a caller to make calls using Internet Protocol (IP) signaling.
In the context of this document, it is focused on the ability to make IP-based 9-1-1 calls. It is the OSP's responsibility to forward 9-1-1 calls toward the serving Emergency Services Network. Since the IP-based OSP is using IP technology, calls destined for an NG Emergency Services Network are not required to go through a gateway, provided that the OSP can deliver calls over

[3] OSPs may interwork calls originated using legacy technologies to IP signaling, however those calls must still go through a gateway to access NG9-1-1-specific interworking functionality. Calls from non-IP enabled endpoint devices must go through a gateway that provides both protocol interworking and NG9-1-1-specific interworking.

an IP-based interface to the serving NG emergency services network using a compatible NG9-1-1 signaling format (e.g., deliver using NENA-i3 compatible SIP interface).

The OSP-IP role may be provided by traditional "phone companies", competitive "phone companies", or other private or public communications entities that are using IP-based technology.

4.1.1.2.3 Legacy Network Gateway (LNG) Operator

The LNG is an NG9-1-1 Functional Element that provides an interface between a non-IP originating network and an NG Emergency Services Network. In this document, the entity that provides the LNG is referred to as the LNG operator. That would typically be the NG9-1-1 System Service Provider (SSP) or the OSP-Legacy. It could also be a government entity or a third party.

4.1.1.2.4 E9-1-1 System Service Provider (E9-1-1SSP) [4]

An E9-1-1SSP provides systems and support necessary to enable 9-1-1 calling for one or more PSAPs in a specific geographic area. Traditionally, the ILEC has provided this role but other models are possible, including arrangements in which the 9-1-1 Authority may choose to operate or outsource pieces of the network.

The E9-1-1SSP role includes providing:

- A method of interconnection for all telecommunications providers, including but not limited to wireline, wireless, and VoIP carriers.
- A method and mechanism for routing a 9-1-1 call to the PSAP with no degradation in service regardless of the technology used to originate the call.
- A method to provide accurate location information for an emergency caller to a PSAP and, if required, to other emergency response agencies.
- For those entities that have responsibility to report to the FCC, a method of capturing outage information and reporting such information via FCC reporting mechanisms.
- Installation of PSAP call handling equipment and training of PSAP personnel when contracted to do so.
- Coordinating with PSAP authorities and other telecommunications entities for troubleshooting and on issues involving contingency planning, disaster mitigation, and recovery.
- Support for Legacy Selective Router Gateway (LSRG) functionality to facilitate the interconnection of legacy Selective Routers with NG Emergency Services Networks.

[4] The roles and responsibilities of a 9-1-1SSP (whether E9-1-1SSP or NG9-1-1SSP) are essentially the same, even though the technology has evolved. As stakeholders continue to work through the implementation details the similarities may change.

4.1.1.2.5 Next Generation 9-1-1 System Service Provider (NG9-1-1SSP) [4]

An NG9-1-1SSP provides systems and support necessary to enable 9-1-1 calling for one or more PSAPs in a specific geographic area. In the past (in E9-1-1) it was typically, but not always, an ILEC. In NG9-1-1, the role is more open to competition, and there are NG Emergency Services Networks in use that are provided by various entities, some of whom specialize in the NG9-1-1SSP role.

The NG9-1-1SSP role includes providing:

- A method of interconnection for all telecommunications providers, including but not limited to wireline, wireless, and VoIP carriers.
- A method and mechanism for routing a 9-1-1 call to the PSAP with no degradation in service regardless of the technology used to originate the call.
- A method to provide accurate location information for an emergency caller to a PSAP and, if required, to other emergency response agencies.
- For those entities that have responsibility to report to the FCC, a method of capturing outage information and reporting such information via FCC reporting mechanisms.
- Installation of PSAP call handling equipment and training of PSAP personnel when contracted to do so.
- Coordinating with PSAP authorities and other telecommunications entities for troubleshooting and on issues involving contingency planning, disaster mitigation, and recovery.

4.1.1.2.6 Legacy Public Safety Answering Point (PSAP) Gateway (LPG) Operator

The LPG is an NG9-1-1 Functional Element that provides an interface between an NG Emergency Services Network and a legacy PSAP.

In this Report, the entity that provides the LPG is referred to as the LPG operator. That would typically be the NG9-1-1SSP or the 9-1-1 Authority/PSAP, but it could be a third party

5 OSP Interconnection to NG9-1-1 Emergency Services Networks

The goal of NG9-1-1 is to provide at least E9-1-1-equivalent functionality in support of emergency call originations from fixed, nomadic, and mobile IP users, and to build on those capabilities to improve performance and extend feature functionality (e.g., to support delivery of text-based emergency services requests to PSAPs). There are a number of alternative NG9-1-1 Service Architectures under discussion in various industry groups. NENA has defined a long-term solution for emergency calling, referred to as the i3 Solution, whose end-state assumes end-to-end IP signaling from an IP-enabled endpoint to an IP-enabled PSAP, with callback and caller location information provided to the PSAP with the call. Similarly, a joint work group in ATIS has defined the architecture, protocol, and procedures to support the processing of emergency calls by an IP Multimedia Subsystem (IMS)-based NG Emergency Services Network. Regardless of the Functional Elements and interfaces that make up these architectures, NG9-1-1 Service Architectures must, at a minimum, support current E9-1-1 capabilities.

A fundamental capability required of any NG Emergency Services Network is the ability to selectively route an emergency call to the appropriate PSAP based on the location from which the call was originated. This implies that information identifying the location of the caller must be available at any routing element in the call path. Emergency call setup in an NG9-1-1 environment is expected to be Session Initiation Protocol (SIP)-based. The SIP signaling associated with an emergency session request is expected to include location information, either "by value" (i.e., as a Presence Information Data Format–Location Object [PIDF-LO]) in the body of the SIP message or "by reference" (where a location reference is included in the SIP signaling and can be dereferenced to obtain the location value/PIDF-LO). The routing element is expected to use a location value to query a call routing function to obtain routing information for the call. The location information used as input to the call routing function can either be in the form of a civic/street address or geo-coordinates. The output of the call routing function is expected to be in the form of a Uniform Resource Identifier (URI).

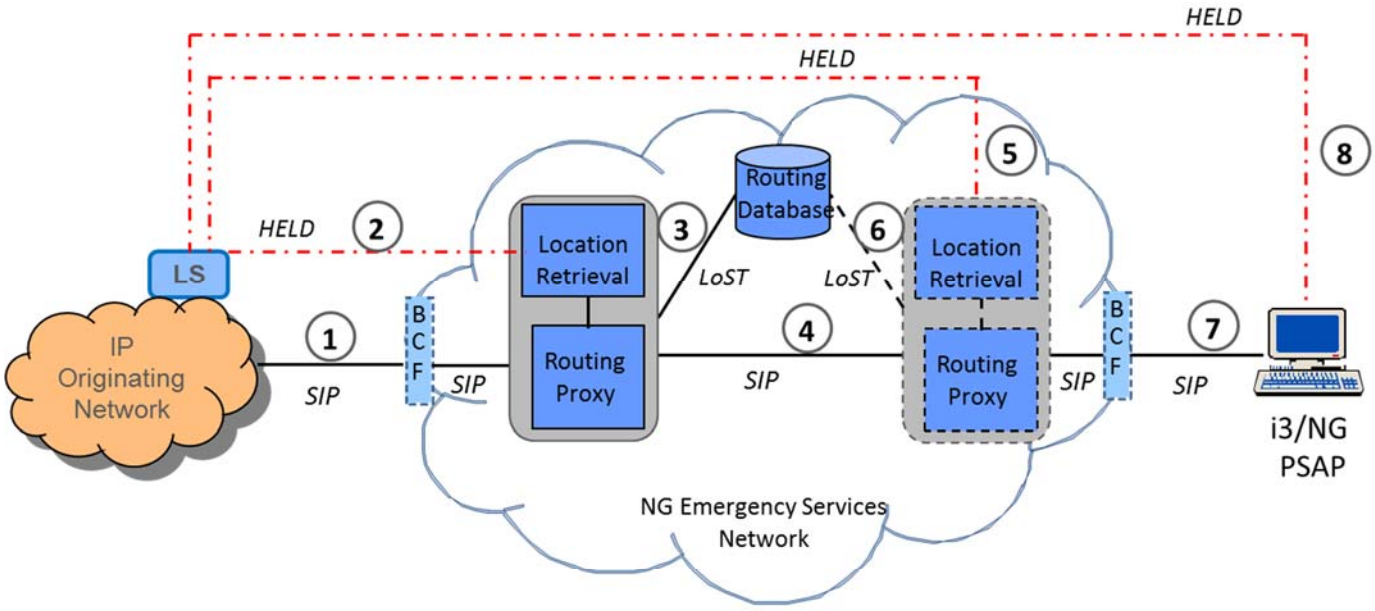
If location-based routing cannot be performed because sufficient information is not received with the call to allow the location-based process to be successful (e.g., location information is not received with the call, or a route cannot be determined for the location value associated with the call), the NG Emergency Services Network must be able to route the call using a default location or default next hop URI (as appropriate for the abnormal condition encountered). Alternate/Overflow routing allows the NG Emergency Services Network to temporarily redirect emergency calls to/toward a pre-designated alternate PSAP(s)/destination(s) (e.g., call center) when the primary PSAP or next hop element is not available to take calls (e.g., due to network/PSAP conditions or other policy).

When the NG Emergency Services Network delivers an emergency call to an NG PSAP, it is expected to generate SIP signaling that includes location information (by-value or by-reference), callback information, and Additional Data (by-value and/or by-reference). The location information that the NG Emergency Service Network signals to an NG PSAP will be the same as the location information that it received in incoming SIP signaling. For example, if a routing element within the NG Emergency Services Network receives location-by-reference in a SIP INVITE message associated with an incoming emergency call, and it dereferences that location reference to obtain a location-by-value with which to query a location-based routing functional element, it will still send the location-by-reference forward in outgoing SIP signaling to/toward the NG PSAP.

Likewise, routing elements in the NG Emergency Services Network may receive Additional Data associated with a call by reference and/or by value in an incoming SIP INVITE message associated with an emergency call. The routing element is expected to pass the Additional Data to/toward the NG PSAP in the same form as it was received. Today, PSAPs receive non-location information, such as class of service information, associated with an emergency call, in the response from the ALI system. PSAPs that receive emergency calls from the NG Emergency Services Network must, at a minimum, have the same type of non-location information available to them as is available in ALI responses today.

5.1 NG9-1-1 Service Architecture – All IP End-State

Figure 2 provides a high-level functional architecture diagram illustrating an end-state (i.e., all-IP) NG9-1-1 Service Architecture and how emergency calls are processed using this architecture.



BCF – Border Control Function
IP – Internet Protocol
LoST – Location to Service Translation
LS – Location Server
NG – Next Generation
PSAP – Public Safety Answering Point
SIP – Session Initiation Protocol

Figure 2 – High-Level NG9-1-1 Functional Service Architecture (All-IP End-State)

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).
2. 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 using the HTTP-Enabled Location Delivery (HELD) dereferencing protocol, as specified in IETF RFC 6753[5] The response from the MPC/GMLC will include initial (typically Phase I) location information.

- If location is received "by-value", this step will be omitted.
- The routing proxy uses the location information received in incoming SIP signaling (location-by-value) or obtained by dereferencing a location-by-reference to query a routing database.
- The routing database is queried using the Location to Service Translation (LoST) protocol.
- The LoST routing query contains location information and an appropriate service identifier (i.e., a service Uniform Resource Name [URN] in the "sos" family).
- The routing response contains the address of the "next hop" in call path, in the form of a Uniform Resource Identifier (URI).

3. The routing proxy forwards the emergency call/session request (with the **same** callback and location information as it received in incoming SIP signaling) to the "next hop" element based on the URI received in the LoST response.
   - The "next hop" element may be the PSAP or it may be another routing proxy in the call path, depending on the way the NG9-1-1 Service Architecture is implemented.
4. If the next hop in the call path is another routing proxy, and the location information was received in incoming SIP signaling "by-reference", the routing proxy will invoke location retrieval functionality within or accessible to it to retrieve a routing location for the call.
   - A HELD dereference request will be sent to the same element (LS) that the first routing proxy queried to get a routing location.
   - If location is received "by-value", this step will be omitted.
5. 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.
6. The routing proxy forwards the emergency call/session request (with the **same** callback and location information as it received in incoming SIP signaling) to the "next hop" element based on the URI received in the LoST response.
   - In this example, the "next hop" is assumed to be the target PSAP for the emergency call.
   - In this example, the target PSAP is assumed to be an i3/NG PSAP.

[5] This example illustrates location dereferencing using the HELD dereferencing protocol. NG9-1-1 standards also allow the use of a SIP-based location dereferencing mechanism.

7. If the location information delivered to the PSAP is a location-by-reference, the PSAP will send a HELD dereference request to the element identified in the location reference (i.e., the LS) to obtain an estimated caller location for the call.

5.2 Transitional/Interworking Architectures in Support of Emergency Calling

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.

The gateway functionality that supports the interconnection of a legacy originating network and an NG Emergency Services Network, referred to by NENA as a Legacy Network Gateway (LNG), must include signaling interworking to convert the incoming Multi-Frequency (MF) or Signaling System Number 7 (SS7) signaling generated by a legacy origination network to the IP-based (i.e., SIP) signaling supported by an NG Emergency Services Network. [6]

In addition, since routing within the NG Emergency Services Network will be based on location, the Legacy Network Gateway on the ingress side of an NG Emergency Services Network must support the ability to use the information provided by a wireline switch or Mobile Switching Center (MSC) in call setup signaling (e.g., calling number/ANI, Emergency Services Routing Key [ESRK], cell site/sector represented by an Emergency Services Routing Digit [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 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.

In addition to gateway functionality on the ingress side of an NG Emergency Services Network, there will be a need to support gateway functionality on the egress side of the NG Emergency Services Network. That is due to the fact that, while an increasing number of PSAPs will evolve to support NG functionality over time, NG Emergency Services Networks must be able to deliver emergency calls to interconnected legacy PSAPs, as well as to legacy Emergency Services Networks.

In regard to interfacing with a legacy PSAP, the NG9-1-1 Service Architecture must include a functional element that will provide signaling interworking and other functionality necessary for emergency calls routed via the NG Emergency Services Network to be delivered to and handled

[6] In some implementations, legacy origination networks may support circuit switch to IP-based signaling, making MF or SS7 interworking to IP based signaling at the LNG unnecessary.

by legacy PSAPs without requiring changes to legacy PSAP Customer Premises Equipment (CPE). That functional element is, defined by NENA as a Legacy PSAP Gateway (LPG).

Calls routed via an NG Emergency Services Network and delivered to a legacy PSAP must undergo signaling interworking to convert the incoming IP-based (i.e., SIP) signaling supported by the NG Emergency Services Network to the Traditional MF or Enhanced MF (E-MF) signaling supported by the legacy PSAP. Functionality must also be applied by the NG Emergency Services Network to emergency call originations to allow the legacy PSAP to experience call delivery, ALI data retrieval, and feature activation the same way as they do today. The LPG handles those functions.

5.2.1 Support for Interconnection of NG Emergency Services Networks & Legacy Originating Networks

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 (LNG) functional element. 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. To support this routing function, the LNG applies NG9-1-1-specific interworking functionality to legacy emergency calls that allows the information provided in the call setup signaling by the wireline switch or MSC (e.g., calling number/ANI, ESRK, ESRD) to be used as input to the retrieval of routing location (in the form of a street address or geo-coordinate location) from an associated location server/database. The LNG uses this location information to query a call routing function to obtain routing information in the form of a URI. The LNG must then forward the emergency call/session request to a routing element in the NG Emergency Services Network, using the URI provided by the call routing function. The LNG will include callback and location information in the outgoing SIP signaling.

The location server/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 caller 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 3 provides a High-Level Functional Architecture diagram illustrating how emergency calls are processed using an interworking architecture involving an LNG.

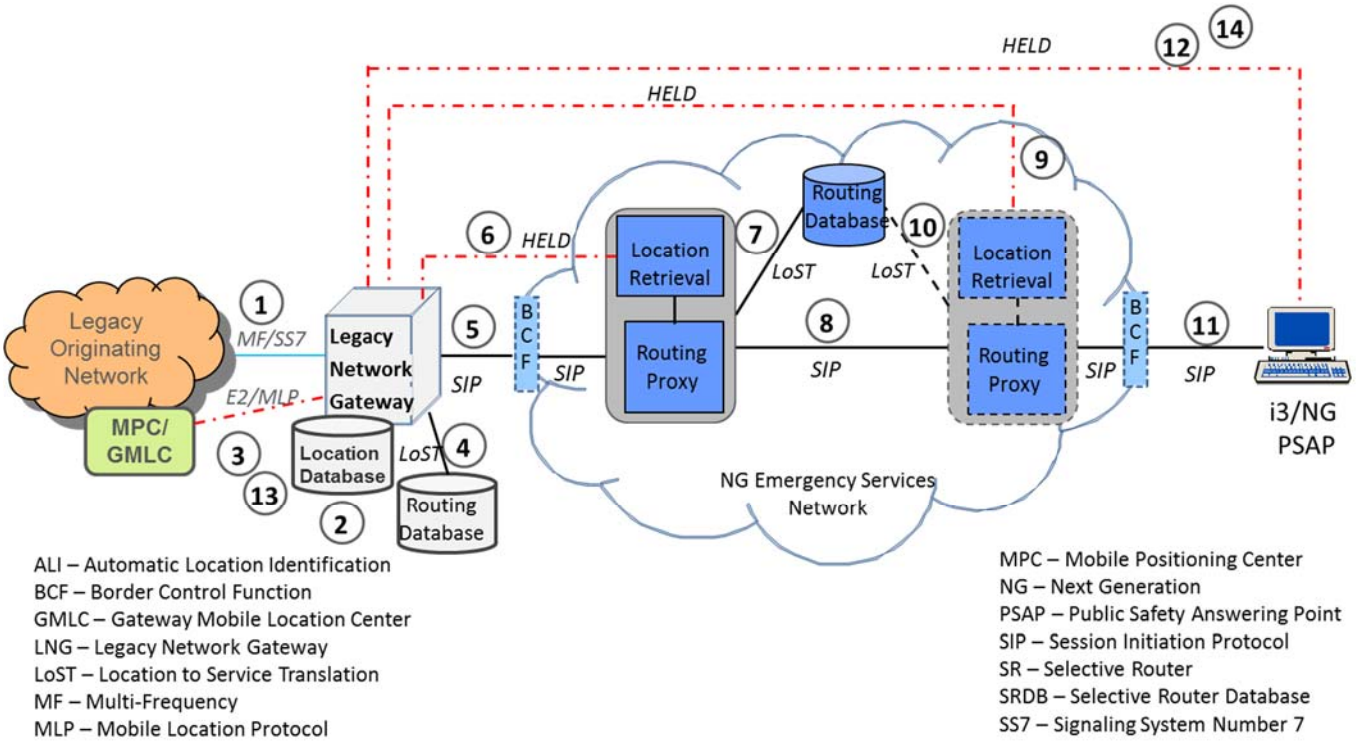


Figure 3 – High-Level NG9-1-1 Service Functional Architecture Involving Legacy Network Gateway

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[7] [8].
   - 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.
2. The LNG will interact with a local location database which will map the calling number/ANI/ESRK/ESRD to a routing location.
3. 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) location information.

[7] Some LNGs may support SIP ingress in addition to MF and SS7.

[8] Legacy Originating Networks may deliver traffic using an aggregation service that interconnects via BCF to the NG Emergency Services Network.

4. The LNG queries a routing database using the routing location obtained in Step 2 using the LoST protocol.
   - 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.
5. 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.
6. If the location information is received "by-reference" the location retrieval functionality within or associated with the routing proxy will be invoked.
   - A HELD dereference request will be sent to the LNG to obtain a routing location for the call; the LNG will return the routing location obtained in Step 2.
   - If location is received "by-value", this step will be omitted.
7. The routing proxy uses the location information received in incoming SIP signaling (location-by-value) or obtained by dereferencing a location-by-reference to query a routing database.
   - The routing database is queried using the LoST protocol.
   - The LoST routing query contains location information and an appropriate service identifier (i.e., a service URN in the "sos" family).
   - The routing response contains the address of the "next hop" in the call path, in the form of a URI.
8. The routing proxy forwards the emergency call/session request (with the same callback and location information as it received in incoming SIP signaling) to the "next hop" element based on the URI received in the LoST response.
   - The "next hop" element may be the PSAP or it may be another routing proxy in the call path, depending on the way the NG9-1-1 Service Architecture is implemented.
9. If the next hop in the call path is another routing proxy, and the location information was received in incoming SIP signaling "by-reference", the routing proxy will invoke location retrieval functionality within or accessible to it to retrieve a routing location for the call.
   - A HELD dereference request will be sent to the LNG, and the LNG will return the routing location obtained in Step 2.
   - If location is received "by-value", this step will be omitted.
10. 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, along with a service URN, to query a routing database using the LoST protocol.

11. The routing proxy forwards the emergency call/session request (with the same callback and location information as it received in incoming SIP signaling) to the "next hop" element based on the URI received in the LoST response.
    - In this example, the "next hop" is assumed to be the target PSAP for the emergency call.
    - In this example, the target PSAP is assumed to be an i3/NG PSAP.
12. If the location information delivered to the PSAP is a location-by-reference, the PSAP will send a HELD dereference request to the LNG to obtain caller location.
13. If the location dereference request from the i3/NG PSAP indicates that initial location should be returned, the LNG will return the initial caller location 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.
14. The LNG returns the updated location information to the i3/NG PSAP.

5.2.2 Support for Interconnection of NG Emergency Services Networks & Legacy Selective Routers

During the transition period while the Emergency Services infrastructure migrates toward IP, and PSAPs evolve to support i3/NG functionality, wireline and wireless callers and PSAPs that are served by legacy Selective Routers (SRs), will need to be supported. A Legacy Selective Router Gateway (LSRG) will provide the needed functionality to facilitate emergency call handling in transitional architectures where legacy SRs and ALIs are still present. The LSRG is a signaling and media connection point between a legacy SR and an NG Emergency Services Network. The LSRG allows emergency originations routed via a legacy SR to terminate on an NG PSAP, as well as allowing calls routed via an NG Emergency Services Network to terminate to a legacy PSAP that is connected to a legacy SR. The LSRG also facilitates transfers of calls between PSAPs that are served by legacy SRs and PSAPs that are served by NG Emergency Services Networks, regardless of the type of network from which the call originated.

This section describes the interconnection of legacy originating networks that continue to be served by legacy SRs with NG9-1-1 Emergency Services Networks via an LSRG on the ingress side of the NG9-1-1 Emergency Services Network. (See *Section 9* for details related to transitional architectures in which LSRGs are used to interconnect NG9-1-1 Emergency Services Networks with legacy PSAPs that are served by Selective Routers).

Calls originating in legacy end offices or MSCs and routed via a legacy SR must undergo signaling interworking to convert the incoming SS7 signaling used by the SR to the SIP-based signaling supported by the NG Emergency Services Network. An LSRG on the ingress side of the NG Emergency Services Network supports an SS7 interface on the SR side, and a SIP interface toward the NG Emergency Services Network. The LSRG must support functionality to interwork the SS7 signaling that it receives from the SR with the SIP signaling used in the NG Emergency Services Network.

The LSRG is also responsible for routing emergency calls that originate in a network that is connected to the SR to the appropriate (routing) element in the NG Emergency Services Network. To support this routing, the LSRG must apply service-specific interworking functionality to legacy emergency calls to allow the information provided by the wireline switch or MSC (e.g., calling number/ANI, ESRK, ESRD) in the call setup signaling, and passed to the LSRG through the SR, to be used as input to the retrieval of routing and caller location. The LSRG obtains caller location information by querying a legacy ALI database using the "key" (i.e., calling number/ANI, ESRK, ESRD) provided in call setup signaling. The LSRG obtains routing location either from the ALI database (e.g., for wireline originations) or by mapping the received ESRK/ESRD to a location that will result in the call being routed to the target PSAP. The LSRG uses the routing location to query a call routing function to obtain routing information in the form of a URI. The LSRG must then forward the emergency call/session request to the appropriate element in the NG Emergency Services Network, based on the URI provided by the routing function. The LSRG includes callback and location information in the outgoing SIP signaling sent to the NG Emergency Services Network.

Figure 4 provides a High-Level Functional Architecture diagram illustrating how emergency calls are processed using a transitional architecture involving an ingress LSRG.

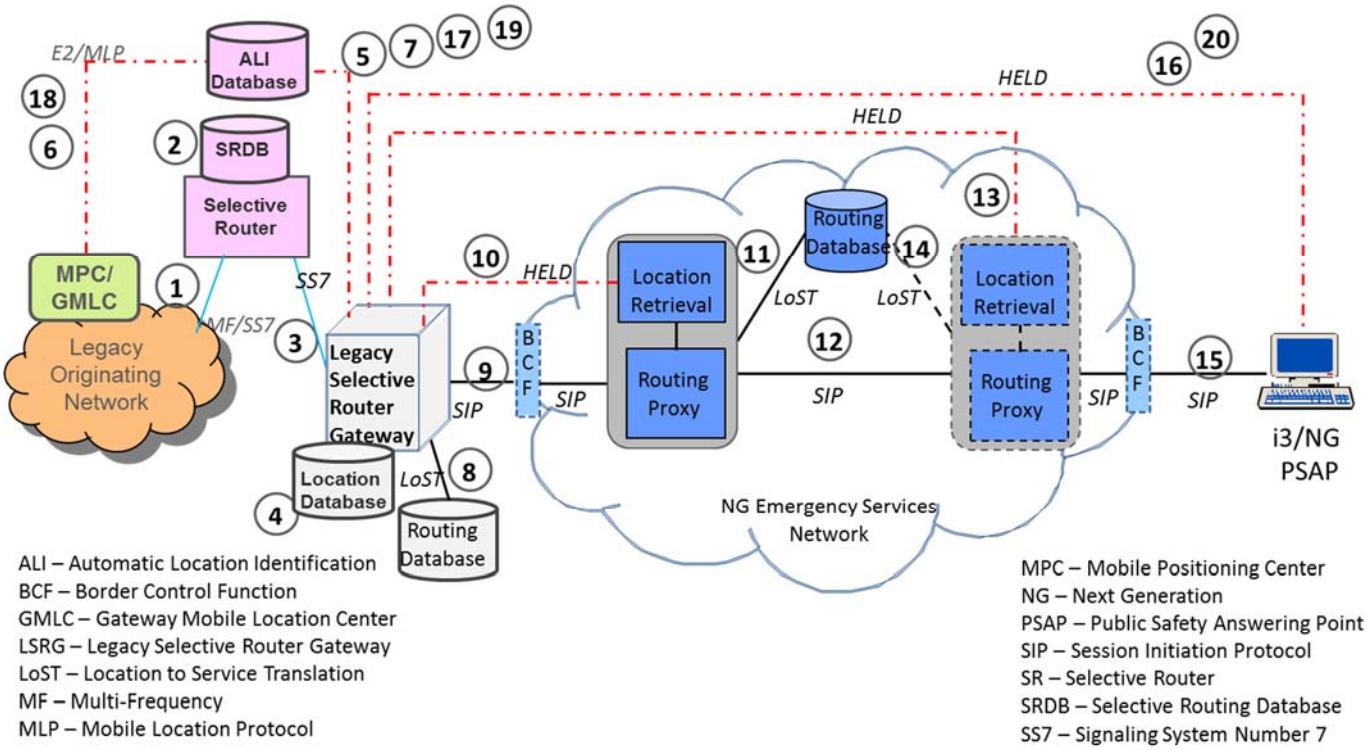


Figure 4 – NG9-1-1 Service Functional Architecture Involving Ingress Legacy Selective Router Gateway

1. A 9-1-1 call is delivered by the legacy originating network to a legacy SR over an MF or SS7 trunk group

- Legacy wireline originations will be delivered with the SS7 Calling Party Number or MF ANI.
- Legacy wireless originations will be 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.

2. The SR queries a Selective Routing Database (SRDB) using the calling number/ANI, ESRK, or ESRD (based on the signaling received over the trunk group from the end office/MSC); the SRDB returns an Emergency Service Number (ESN) that points to a trunk group to an LSRG.
3. The SR delivers the emergency call to the LSRG over an SS7-supported trunk group.
   - The SS7 signaling will include the information (i.e., calling number/ANI, ESRK, ESRD) that the SR received from the end office/MSC.
4. The LSRG interacts with a local location database that maps the calling number/ANI/ESRK/ESRD to a routing location.
5. The LSRG also sends a query to the ALI system requesting caller location for the emergency call.
6. If the call is a legacy wireless emergency call, the ALI will 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) location information.

Note that this step is omitted if the call is from a legacy wireline caller.

7. The ALI system then returns the caller location information to the LSRG.
8. The LSRG queries a routing database using the routing location obtained in Step 4 and an appropriate service URN and receives the address of a routing proxy in the NG Emergency Services Network in response.
9. The emergency call is delivered by the LSRG (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 4 will typically be delivered “by-value” and will be in the form of a civic location/street address; the callback number will be populated with the information received in the SS7 Calling Party Number parameter.
   - 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; the callback number will either be populated with the content of the SS7 Calling Party Number parameter (if both a calling number and an ESRD/ESRK was provided in the signaling from the SR), or with the callback number obtained from the MPC/GMLC (if only an ESRK was provided in call setup signaling from the SR).
10. If the location information is received by the routing proxy “by-reference”, the location retrieval functionality within or accessible to the routing proxy will be

964 invoked. A HELD dereference request will be sent to the LSRG to obtain a routing
965 location for the call; the LSRG will return the routing location obtained in Step 4.

966 If location is received "by-value", this step will be omitted.

967 11. The routing proxy uses the location information received in incoming SIP signaling
968 (location-by-value), or obtained by dereferencing a location-by-reference, to query a
969 routing database.
970 • The routing database is queried using the LoST protocol.
971 • The LoST routing query contains location information and an appropriate service
972 identifier (i.e., a service URN in the "sos" family).
973 • The routing response contains the address of the "next hop" in call path, in the
974 form of a URI.
975 12. The routing proxy forwards the emergency call/session request (with the **same**
976 callback and location information as it received in incoming SIP signaling) to the
977 "next hop" element based on the URI received in the LoST response.
978 • The "next hop" element may be the PSAP or it may be another routing proxy in the call
979 path, depending on the way the NG9-1-1 Service Architecture is implemented.
980 13. If the next hop in the call path is another routing proxy, and the location information
981 was received in incoming SIP signaling "by-reference", the routing proxy will invoke
982 location retrieval functionality within or accessible to it to retrieve a routing location
983 for the call. That is, the routing proxy will send a HELD dereference request to the
984 LSRG, and the LSRG will return the routing location obtained in Step 4.

985 If location is received "by-value", this step will be omitted.

986 14. If present in the call path, the routing proxy will use the location information
987 received in incoming SIP signaling (location-by-value) or obtained by dereferencing
988 a location-by-reference, and a service URN, to query a routing database using the
989 LoST protocol.
990 15. The routing proxy forwards the emergency call/session request (with the **same**
991 callback and location information as it received in incoming SIP signaling) to the
992 "next hop" element based on the URI received in the LoST response.
993 • In this example, the "next hop" is assumed to be the target PSAP for the emergency call,
994 and the target PSAP is an i3/NG PSAP.
995 16. If the location information delivered to the PSAP is a location-by-reference, the
996 PSAP will send a dereference request to the LSRG to obtain caller location.
997 17. If the location dereference request from the i3/NG PSAP indicates that initial
998 location should be returned, the LSRG will return the initial caller location
999 information obtained in Step 7.

1000 If the location dereference request from the i3 NG/PSAP indicates that updated location should
1001 be returned, the LSRG will send a query to the ALI system requesting caller location.

1002 18. If the ALI receives a rebid request from the LSRG, the ALI will send an E2 or MLP
1003 query to the MPC/GMLC requesting updated (i.e., Phase II) location.
1004 19. The ALI returns the content of the MPC/GMLC response to the LSRG.
1005 20. The LSRG returns the updated location information to the i3/NG PSAP.

6 NG9-1-1 Emergency Services Network Interconnection with Legacy PSAPs

6.1 Transitional NG9-1-1 Service Architectures Involving Legacy PSAP Gateways

In addition to supporting the delivery of emergency calls to NG PSAPs, NG Emergency Services Networks are required to support the delivery of emergency calls to legacy PSAPs. To support the delivery of emergency calls that are routed via NG Emergency Services Networks to a legacy PSAP, NG9-1-1 Service Architectures include a Legacy PSAP Gateway (LPG) that serves as the signaling and media interconnection point between the NG Emergency Services Network and the legacy PSAP. The LPG is expected to provide special processing of the information received in incoming (SIP-based) call setup signaling to facilitate call delivery to legacy PSAPs, to assist legacy PSAPs in obtaining the callback and location information necessary to handle the call and support the dispatch of emergency personnel, and to support feature functionality currently available to legacy PSAPs, such as call transfer. The SIP signaling delivered to an LPG by an NG Emergency Services Network will contain the same information as the SIP signaling that is delivered to an NG PSAP, including location information (by-reference or by-value) and callback information. The LPG will be responsible for interworking the SIP signaling to the Traditional MF or E-MF signaling that is appropriate for the interface over which the call will be delivered to the legacy PSAP. Traditional MF and E-MF interfaces to legacy PSAPs assume that callback information signaled to a PSAP will be in the form of a 7/10-digit North American Numbering Plan (NANP) number. It is possible that the callback information delivered to an LPG with an emergency call (e.g., associated with a VoIP origination) will not be in the form of (or easily converted to) a 10-digit NANP number. If a PSAP is expecting to receive callback information delivered with the call in call setup signaling, and the callback information received by the LPG is not in the form of (or easily converted to) a 10-digit NANP number with an NPA that is appropriate for the target PSAP (i.e., consisting of one of four NPAs supported by a legacy PSAP that supports a Traditional MF interface), the LPG will perform a mapping from the callback information to a locally significant digit string that can be delivered to the legacy PSAP via Traditional MF or E-MF signaling (as appropriate for the PSAP). The locally significant digit string delivered to the PSAP will be of the form "NPD/NPA-511-XXXX". The LPG will use the same mechanism to map callback information to a locally significant digit string if the callback information received in call setup signaling is in the form of a 10-digit NANP number, but the NPA is not one that is supported by the PSAP.

Location information received by the LPG will be provided to the legacy PSAP outside of the call setup process via a legacy ALI interface. The LPG will look to the legacy PSAP like an ALI system and the legacy PSAP will query the LPG using the same interface as it would use to query an ALI database. Like an ALI system, when an LPG is queried with an ALI location key (i.e., callback number and/or pANI), the LPG will respond with the location and other non-location information, as appropriate for the query protocol used by the legacy PSAP. If the SIP signaling associated with an emergency call routed via the NG Emergency Services Network contains a location by value, the LPG will include that location information in the ALI response, formatted appropriately for the receiving PSAP. If the SIP signaling delivered by the

NG Emergency Services Network to the LPG includes a location-by-reference, the LPG must first dereference the location-by-reference to obtain the location information to return to the PSAP in response to an ALI query.

If the PSAP expects to receive location information (i.e., a location key) delivered with the emergency call, the LPG will generate a 10-digit key (pANI) and associate it with the location and other call information that was provided in the incoming SIP INVITE message from the NG Emergency Services Network. This pANI will be passed to the PSAP via the Traditional MF or E-MF interface (as appropriate for the PSAP) and will be used by the PSAP in the ALI query that it generates. If the PSAP expects to receive both callback and location information with the emergency call (i.e., via an E-MF interface) and a pANI of the form NPD/NPA-511-XXXX is sent in the MF sequence corresponding to the callback number, the same digit string can be generated by the LPG and delivered to the legacy PSAP as a pANI that represents the location information received by the LPG in incoming signaling.

Note that, like emergency calls from non-initialized mobile devices, legacy PSAPs will not be able to initiate a callback call if the callback information associated with the emergency call is not in the form of a NANP number.

Figure 5 provides a High-Level Functional Architecture diagram illustrating how emergency calls are processed using an interworking architecture involving an LPG.

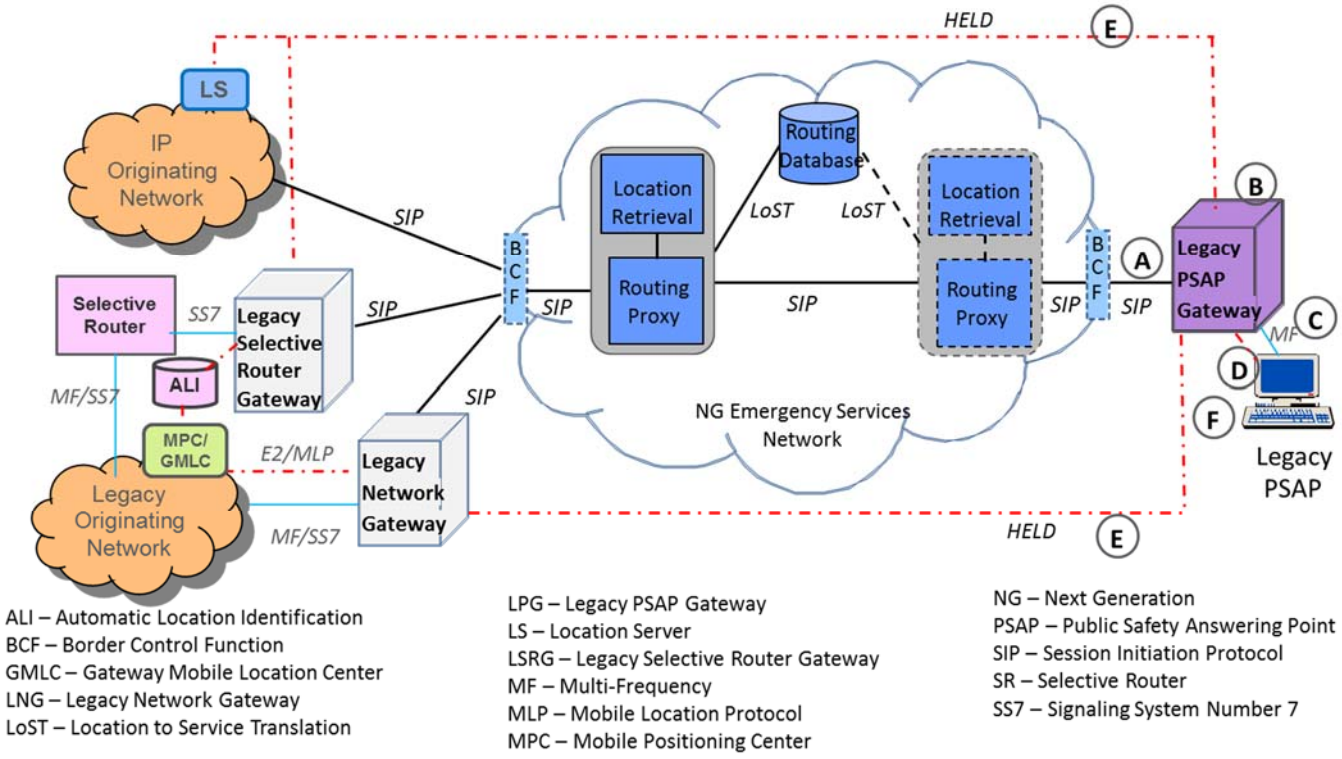


Figure 5 – NG9-1-1 Service Functional Architecture Involving Legacy PSAP Gateway

An emergency call originates in an IP originating network or legacy originating network and proceeds as described above to the point where a routing URI associated with the PSAP is obtained by a Routing Proxy. The emergency call, and associated data, is then processed as follows:

A. The routing proxy forwards the emergency call/session request (with the **same** callback and location information as it received in incoming SIP signaling) via a BCF toward the legacy PSAP identified in the URI received in the response from the Routing Database.
   - The routing proxy forwards the SIP INVITE message to an LPG that is appropriate for the PSAP URI (i.e., an LPG to which the PSAP URI obtained from the routing database resolves).

B. Upon receiving the emergency session request from the routing proxy, the LPG performs the following functions:
   - The LPG determines the type of interface supported by the target legacy PSAP.
     - Call delivery to legacy PSAPs is typically via a Traditional MF or E-MF interface.
       - A Traditional MF interface involves the signaling of an MF ANI sequence that consists of a Numbering Plan Digit (NPD) and a 7-digit ANI, where the value of the NPD represents one of four NPAs as well as an indication whether the ANI should be displayed using a steady display or a flashing display.
       - An E-MF interface supports the delivery of a 10-digit ANI with two ANI II digits and, optionally, a second 10-digit number (typically a pANI that represents the cell site/sector from which a legacy wireless call originated); the II digits indicate how the ANI should be displayed (i.e., steady or flashing).
   - If the PSAP supports a Traditional MF interface or an E-MF interface that only supports the delivery of one 10-digit number, the LPG will determine, based on per-PSAP provisioning, whether callback information or location information (i.e., a location key) should be signaled to the PSAP.
   - If the LPG determines that callback information is to be signaled to the PSAP, the LPG will inspect the callback information to see if it is in the form of (or easily converted to) a 10-digit NANP number.
     - If callback information is to be delivered, and the callback information received in incoming SIP signaling is in the form of (or easily converted to) a 10-digit NANP number, and the NPA associated with that number is one that is appropriate for the target PSAP (i.e., one that can be mapped to an NPD digit), the LPG will use the received information to populate the 10-digit ANI signaled via E-MF or the NPD + 7-digit ANI sent via Traditional MF to the PSAP.
     - If callback information is to be delivered, and the callback information received in the incoming SIP signaling is NOT in the form of (or easily converted to) a 10-digit NANP number (or if the callback information is in the form of a 10-digit NANP number, but the NPA is not one that can be

mapped to an NPD that is supported by a legacy PSAP via a Traditional MF interface), the LPG will generate a substitute ANI digit string of the form NPA-511-XXXX (for the E-MF case) or NPD + 511-XXXX (for the Traditional MF case, where the NPD is associated with an NPA that is appropriate for the target PSAP).

- If the PSAP supports an E-MF interface, it supports the delivery of two 10-digit numbers and either callback or location information is not available, the LPG will signal the digits "000-9-1-1-0000" for the missing information.
- If the LPG determines that location information is to be signaled to the PSAP, the LPG will generate a location key that is also of the form NPA-511-XXXX (for the Enhanced MF case) or NPD + 511-XXXX (for the Traditional MF case).

C. The LPG delivers the emergency call to the PSAP using Traditional or E-MF signaling, as appropriate for the target PSAP.
D. The PSAP uses the information provided via MF (i.e., the ANI and/or location key) to query the LPG as if it were a legacy ALI system.
E. If the location information received by the LPG in incoming SIP signaling is "by-reference", the LPG will send a HELD dereference request to the element identified in the location reference (i.e., the LS in an IP originating network, or an LNG or an LSRG) to obtain a location value.
   - Note that this step will be omitted if the location information received by the LPG in incoming SIP signaling was "by-value".
F. The LPG sends a response to the ALI request from the legacy PSAP that contains location information, callback information, and other non-location information (e.g., class of service, Service Provider contact information).

6.2 Transitional NG9-1-1 Service Architectures to Support Interconnection with Legacy PSAPs that are Served by Legacy Selective Routers

An emergency call that is routed via an NG Emergency Services Network and is destined for a legacy PSAP that is connected to an SR must traverse an LSRG on the egress side of the NG Emergency Services Network. Upon receiving an emergency session request from an NG Emergency Services Network, the LSRG will analyze the signaled information and apply NG9-1-1-specific processing to identify the outgoing trunk group over which the call will be delivered to the interconnected legacy SR, and to ensure that the information delivered to the legacy SR is in an acceptable format. The LSRG will select the outgoing route to the SR based on the destination PSAP number/address provided in the incoming SIP signaling from the NG Emergency Services Network. The LSRG will maintain a mapping between the PSAP URI delivered to it in incoming SIP signaling and the Directory Number (DN) of the corresponding PSAP on the SR. The LSRG delivers the emergency call to the SR over an SS7-supported tandem-to-tandem trunk group. SS7 interfaces to legacy SRs assume that the PSAP DN and the callback information and/or location keys (i.e., pANIs) signaled to the legacy SR will be in the form of a 10-digit NANP number. It is possible that some emergency originations (e.g., from VoIP callers) will contain callback information that is not in the form of (or easily converted to)

a 10-digit NANP number. If callback information is to be delivered to the SR (i.e., in the SS7 Calling Party Number parameter) and it is not in the form of (or easily converted to) a 10-digit NANP number, the LSRG will perform a mapping from the non-NANP callback information to a pseudo callback number that is appropriate for the destination PSAP.

The LSRG will also need to be able to pass a key to the location information associated with the emergency call to the SR, either by itself (i.e., populated in the SS7 Calling Party Number parameter) or in addition to the callback information (where the callback information will be populated in the SS7 Calling Party Number parameter and the location key will be populated in the SS7 Generic Digits Parameter). An egress LSRG must therefore also generate a 10-digit pANI to associate with the location information received in incoming signaling from the NG Emergency Services Network. (Note that the same digit string can be used to represent both the callback and location information.)

If the SR receives both a callback number (or pseudo callback number) and a pANI (associated with the location information), it will use per-PSAP provisioning to determine what will be signaled forward to the PSAP. The PSAP will use the information received in incoming signaling to query an ALI system to obtain caller location for the call. The ALI will steer the location query back to the LSRG, in the same way as it would steer a location query to an MPC/GMLC in a wireless originating network. To support location delivery to legacy PSAPs that are served by legacy SRs, the LSRG must support the interface protocol used by the interconnected ALI system to query an MPC/GMLC. The location key used in the query to the LSRG will be the pANI (possibly in combination with the callback number/pseudo callback number) created by the LSRG for the emergency call. If the location information received from the NG Emergency Services Network is in the form of a location-by-value, the LSRG will be responsible for returning that location information, as well as the callback number and other non-location information, in the response to the ALI system. If the location information is in the form of a civic location/street address, the LSRG must ensure that location returned in the ALI response is in a format that is acceptable to the ALI system/PSAP. If the location information received by the NG Emergency Services Network is in the form of a location-by-reference, the LSRG will first have to dereference the location reference to obtain the location value to be returned in the response to the ALI system. Once again, if the location value is in the form of a civic location/street address, the LSRG will have to ensure that location returned in the ALI response is in an acceptable format.

Figure 6 provides a High-Level Functional Architecture diagram illustrating how emergency calls are processed using a transitional architecture involving an egress LSRG.

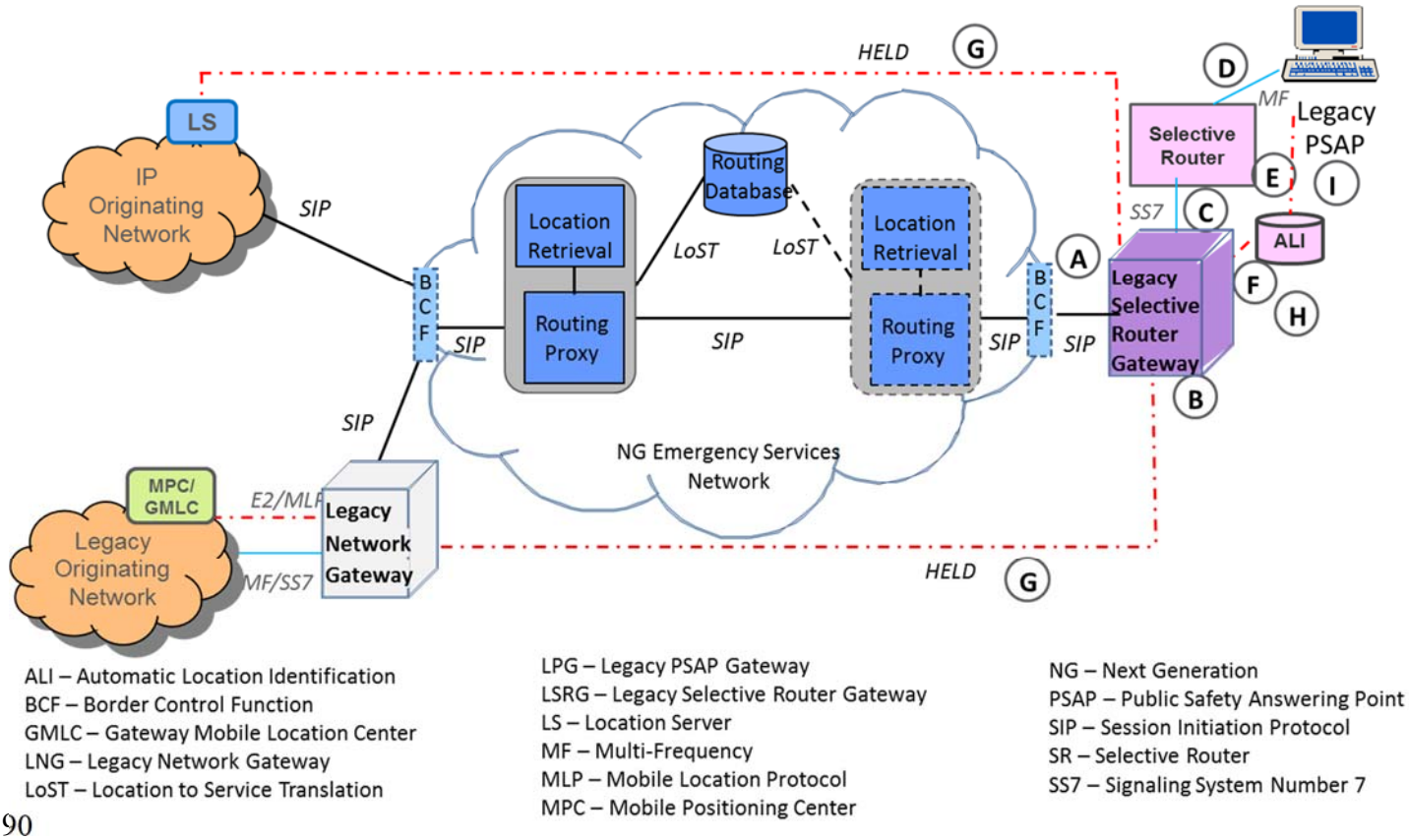


Figure 6 – NG9-1-1 Service Functional Architecture Involving Egress Legacy Selective Router Gateway

An emergency call originates in an IP originating network or legacy originating network and proceeds as described in the previous diagrams to the point where the routing URI associated with the PSAP is obtained by a Routing Proxy. The emergency call, and associated data, is then processed as follows:

A. The routing proxy forwards the emergency call/session request (with the same callback and location information as it received in incoming SIP signaling) via a BCF toward the legacy PSAP identified in the URI received in the response from the Routing Database.
   - In this scenario, the target PSAP is a legacy PSAP that is still being served by a Selective Router.
   - The routing proxy forwards the SIP INVITE message to an LSRG that is appropriate for the PSAP URI (i.e., an LSRG to which the PSAP URI obtained from the routing database resolves).

B. Upon receiving the emergency session request from the routing proxy, the LSRG performs the following functions:
   - The LSRG determines, based on provisioning, what information should be sent over the SS7-supported trunk group to the SR that serves the target PSAP.

- The trunk group supports the delivery of a single 10-digit number (i.e., which will be populated in the SS7 Calling Party Number parameter) in addition to the PSAP directory number sent in the SS7 Called Party Number parameter.
- The trunk group supports the delivery of two 10-digit numbers (i.e., one of which will be populated in the SS7 Calling Party Number parameter and the other in the SS7 Generic Digits Parameter) in addition to the PSAP directory number sent in the SS7 Called Party Number parameter.

- In either case, the LSRG will associate an ESN-appropriate pANI with the location information received in incoming SIP signaling from the routing proxy.
- If the LSRG determines that callback information is to be signaled to the SR along with the pANI/location key, the LSRG will inspect the callback information to see if it is in the form of (or easily converted to) a 10-digit NANP number.
  - If callback information is to be delivered, and the callback information received in incoming SIP signaling is in the form of (or easily converted to) a 10-digit NANP number, the LSRG will use the received information to populate the SS7 Calling Party Number parameter.
  - If callback information is to be delivered, and the callback information received in the incoming SIP signaling is NOT in the form of (or easily converted to) a 10-digit NANP number, the LSRG will generate a "pseudo callback number" (which may have the same value as the pANI described above) to populate in the SS7 Calling Party Number parameter.

C. The LSRG routes the call to the legacy Selective Router over an SS7-supported trunk group.
D. The Selective Router queries the SRDB (not shown) to obtain an ESN for the call (for potential use in Selective Transfer), and delivers the emergency call to the PSAP using Traditional or Enhanced MF signaling, as appropriate for the target PSAP.
E. The PSAP uses the information provided via MF (i.e., the ANI and/or location key) to query the legacy ALI system.
F. The ALI system steers the location query to the LSRG (as if it were an MPC/GMLC), using either the E2 protocol or MLP.
G. If the location information received by the LSRG in incoming SIP signaling is "by-reference", the LSRG will send a HELD dereference request to the element identified in the location reference (i.e., the LS in an IP originating network, or an LNG) to obtain a location value.

Note that this step will be omitted if the location information received by the LSRG in incoming SIP signaling was "by-value".

H. The LSRG sends a response to the ALI that contains location information, callback information, and other non-location information (e.g., class of service, Service Provider contact information) as appropriate for the E2/MLP interface.

I. The ALI sends a response to the PSAP that contains location information, callback information, and other non-location information, as appropriate for the interface protocol used between the ALI and the PSAP.

7 IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination

ATIS-0700015 [2] defines the functional interconnection of an originating IMS network to Emergency Services Networks, as shown in Figure 7. The scope of this standard is to identify, and adapt as necessary, 3GPP Common IMS emergency procedures for applicability in North America to support emergency communications originating from an IMS subscriber (fixed, nomadic, or mobile) and delivered to an Emergency Services IP network (ESInet) or to a legacy Selective Router.

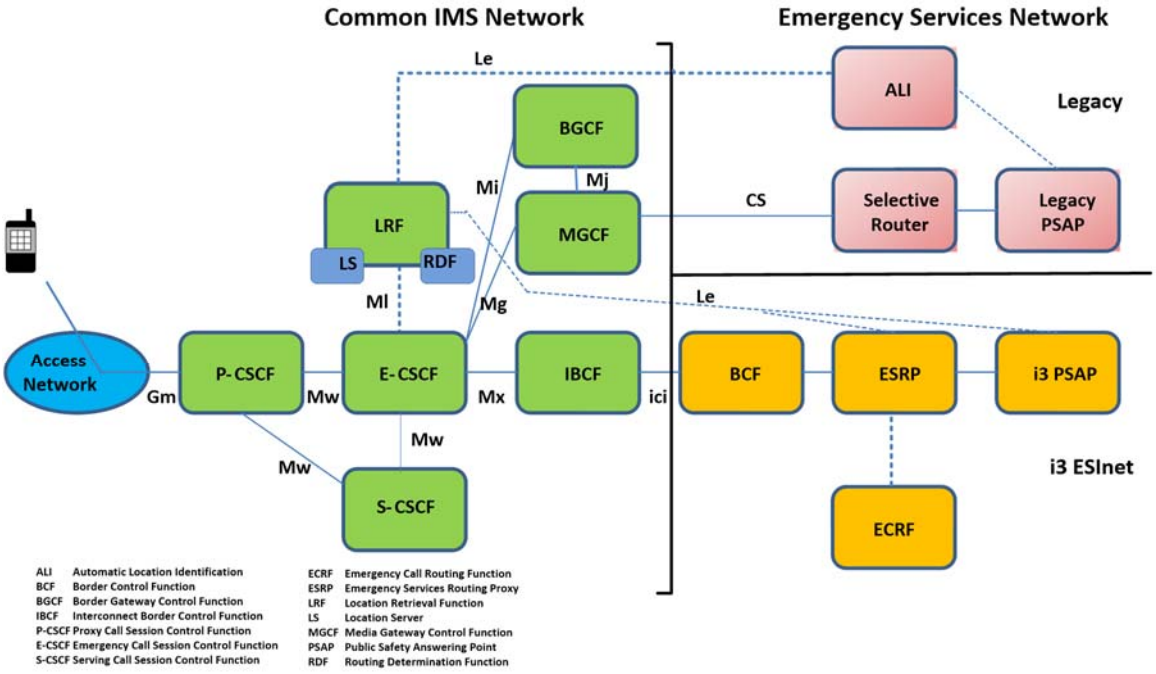


Figure 7 – ATIS 0700015 IMS Interconnection Architecture

In the North American architecture, the emphasis is on the relationship between the originating IMS network and the interconnected Emergency Services Network, rather than the PSAP. For example, emergency calls destined for legacy PSAPs may be directed from the originating IMS

network to a Selective Router in a legacy Emergency Services Network or to an Emergency Services IP Network (ESInet) that hosts legacy PSAPs. Emergency calls destined for IP-capable PSAPs are directed from the originating IMS network to an ESInet. Thus, in North America, it is the capabilities of the interconnected Emergency Services Network that influence call handling within the IMS originating network, rather than the specific capabilities of the PSAP to which the call will ultimately be delivered.

For calls to a NENA i3 ESInet, calls may be delivered with the location of the caller (referred to as location-by-value [LbyV]) or a location reference URI or Reference Identifier (referred to as location-by-reference [LbyR]). If the call is delivered to the ESInet with location information that is in the form of a Reference Identifier, routing elements within the ESInet will use the Reference Identifier to query the originating IMS Network for the routing location. NG/i3 PSAPs (or gateways on behalf of legacy PSAPs) will also use the Reference Identifier to obtain caller location after the call has reached the PSAP.

If the originating IMS Network needs to acquire location information, the Location Retrieval Function (LRF) within the originating IMS network may do so by accessing a Location Server (LS). The characteristics of the LS may differ based upon the class of service. For example, for mobile calls, the originating IMS Network may query location determination equipment via the LS.

Once the originating IMS Network has obtained location, it must select the appropriate Emergency Services Network to deliver the call to. The LRF may access an integrated Routing Determination Function (RDF) or interrogate an external RDF to obtain routing information for the emergency call.

7.1 IMS Functional Elements

The following definitions describe the IMS Functional Elements shown in Figure 7 above. See ATIS-0700015 [2] for further details about the elements and interfaces illustrated in Figure 7.

7.1.1 User Equipment (UE)

The UE initiates the emergency session establishment request.

7.1.2 Proxy Call Session Control Function (P-CSCF)

The P-CSCF receives the emergency session establishment request from the UE, detects that it is an emergency session request, and forwards it to the E-CSCF. Based on the operator policy, in some situations the P-CSCF may forward the emergency session establishment request to the S-CSCF.

7.1.3 Emergency Call Session Control Function (E-CSCF)

The E-CSCF receives the emergency session establishment request from the P-CSCF, obtains location information via the LRF, obtains routing information from the LRF, and forwards the emergency session establishment request per the routing information.

7.1.4 Serving Call Session Control Function (S-CSCF)

The Serving Call Session Control Function may be in the call path prior to the E-CSCF.

7.1.5 Location Retrieval Function (LRF)

The LRF retrieves location information for a UE and obtains routing information for an emergency session of the UE from the Routing Determination Function (RDF).

7.1.6 Routing Determination Function (RDF)

The RDF provides routing information for an emergency session.

7.1.7 Media Gateway Control Function (MGCF)

The Media Gateway Control Function (MGCF) interworks calls between the Common IMS network and the legacy Emergency Services Network

7.1.8 Location Server (LS)

The Location Server acquires the UE location if necessary.

7.1.9 Breakout Gateway Control Function (BGCF)

The Breakout Gateway Control Function (BGCF) manages call control to the MGCF.

7.1.10 Interconnecting Border Control Function (IBCF)

The Interconnection Border Control Function (IBCF) Provides IP connectivity to the i3 ESInet.

7.2 IMS Reference Points

Details regarding the Reference Points used in Figure 7 and elsewhere in this Report can be found in the following documents.

- For the following IMS Reference Points; Gm, Mw, Mx, Ml, Mi, Mg, Mj and ici see 3GPP TS 23.002 [19].
- For the following IMS Reference Points; Gm, Le and CS see ATIS-0700015 [2]

8 Demarcation Points that may be used in Assessing Risks and Defining Metrics

In an NG9-1-1 environment, the originating network only has visibility into the demarcation points at the boundaries of the Emergency Services Network through which it is interconnected, but not directly into the PSAP. The Emergency Services Network (including the LPG) has visibility directly into the PSAP for call delivery, including the delivery of location keys and callback numbers in call setup signaling. Only the LPG is aware of what data is exchanged between the PSAP and the external data sources (e.g., Location Information Server [LIS], LRF, etc.). In NG9-1-1 scenarios, the originating network will be able to determine whether location and a callback number are delivered to the Emergency Services Network, but will not be able to

determine whether, or in what form, that information is presented to the PSAP. This section analyzes where failures in call and data delivery may be detected in an NG9-1-1 environment.

Figure 8 illustrates the NG9-1-1 environment where calls from legacy networks are delivered to an LNG to be routed toward the PSAP, and IP-based originating networks (e.g., IMS and generic IP-based networks) deliver native SIP requests to the Emergency Services Network to be routed toward the PSAP. The figure illustrates potential points of demarcation (e.g., Demarc 1) that denote the logical boundaries of responsibility between providers. The figure applies the concept of demarcation points, as defined in NENA-INF-003 [9], to the NG9-1-1 environment. It also shows interfaces between different network elements: 1) between an originating network and the Emergency Services Network; 2) within the Emergency Services Network; and 3) between the Emergency Services Network and the PSAP CPE (associated with both legacy and NG9-1-1 PSAPs).

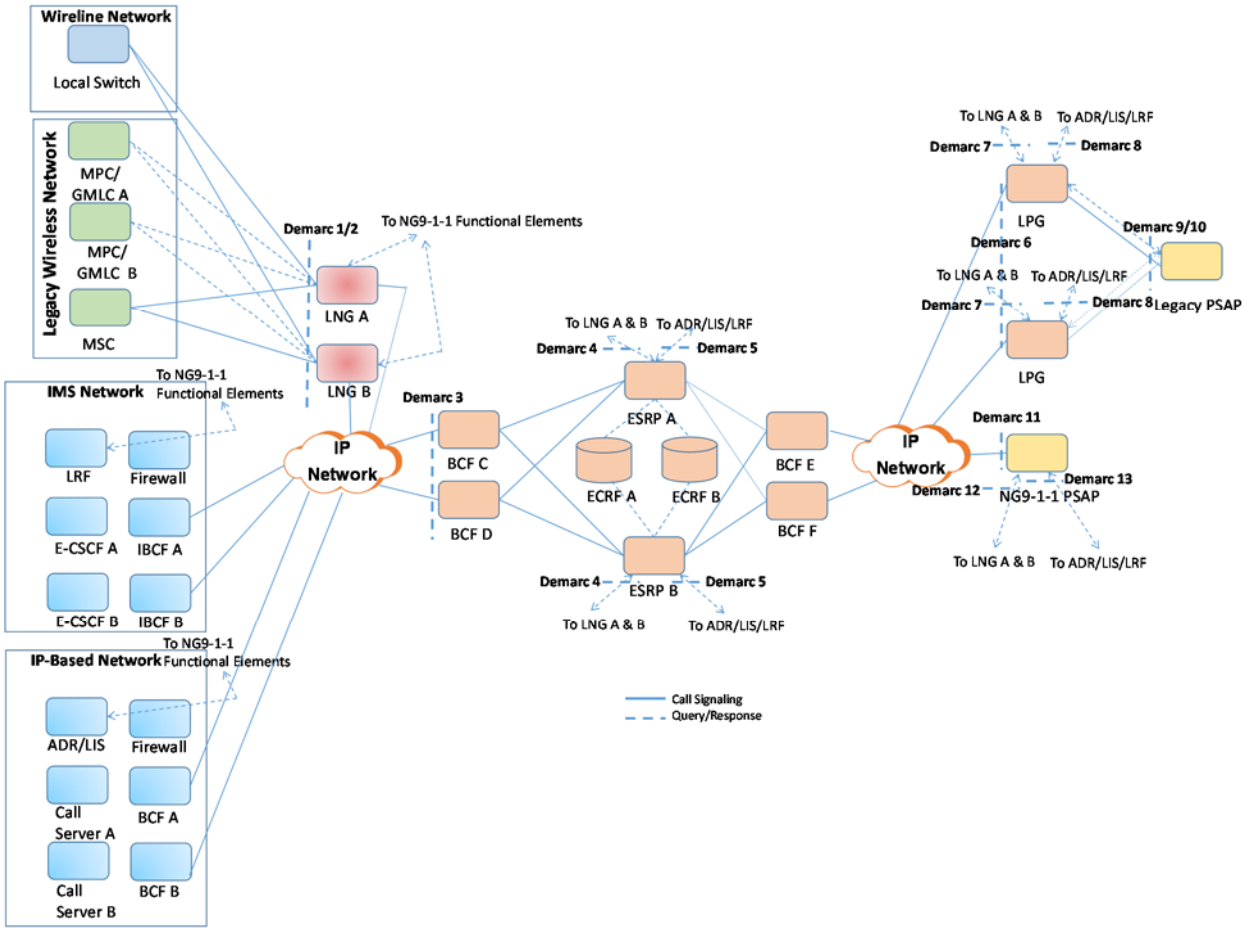


Figure 8 - Legacy OSE to NG9-1-1 Environment

8.1 Demarcation Points

Figure 8 illustrates demarcation points between network providers that denote where responsibility lies for managing and reporting failures.

8.1.1 Demarc 1

This demarcation point applies if the LNG is operated by the NG9-1-1 Service Provider. It is between the LNG and a legacy originating network routing function (e.g., a Local Switch or MSC) and is at the "port" of the LNG.

8.1.2 Demarc 2

This demarcation point applies if the LNG is operated by the NG9-1-1 Service Provider. It is between LNG and the legacy wireless originating network location server (i.e., MPC/GMLC). The originating carriers provide a connection to the data centers that host the LNG.

8.1.3 Demarc 3

This demarcation point is between the IP-based originating network Border Control Function and the Emergency Services Network Border Control Function for routing control. If the LNG is operated by any entity besides the NG9-1-1 Service Provider (e.g., the Originating Service Provider), this demarcation point is between the LNG and the Emergency Services Network BCF. The demarcation is at the ingress of the Emergency Services Network BCF.

8.1.4 Demarc 4

This demarcation point applies if the LNG is operated by any entity besides the NG9-1-1 Service Provider. If the location and/or the Additional Data is sent by reference, the ESRP will query the LNG for it. The demarcation is at the ESRP (note firewalls are included in the path, but not shown).

8.1.5 Demarc 5

This demarcation point is between the ESRP and the location server in an IP-based originating network (e.g., LIS or LRF) and/or the Additional Data Repository (ADR) in an IP-based originating network. The demarcation is at the ESRP (note firewalls are included in the path, but not shown).

8.1.6 Demarc 6

This demarcation point applies if the LPG is *not* operated by the NG9-1-1 Service Provider. The demarcation point is at the ingress of the LPG (note that the LPG may have an additional BCF, not shown).

8.1.7 Demarc 7

This demarcation point applies if the LPG and LNG are *not* operated by the same provider. The LPG would query the LNG for location and Additional Data if they were provided by reference.

8.1.8 Demarc 8

This demarcation point is between the LPG and the location server (e.g., LIS or LRF) and/or the ADR in an IP-based originating network. The demarcation is at LPG (note firewalls are included in the path, but not shown).

8.1.9 Demarc 9

This demarcation point is between the LPG and legacy PSAP to deliver calls over TDM circuits. The demarcation is at the PSAP CPE. This demarcation point applies if the LPG is operated by the NG9-1-1 Service Provider.

8.1.10 Demarc 10

This demarcation point is between the LPG and legacy PSAP to provide legacy ALI-equivalent data (location information and additional data). The demarcation is at the PSAP CPE. This demarcation point applies if the LPG is operated by the NG9-1-1 Service Provider.

8.1.11 Demarc 11

This demarcation point is between ESRP (via the BCF) and the NG9-1-1 PSAP to deliver the call request. It is at the PSAP CPE (note a BCF may be included at the PSAP, but not shown).

8.1.12 Demarc 12

If the location and/or the Additional Data is sent by reference, the NG9-1-1 PSAP will query the LNG for it. The demarcation is at NG9-1-1 PSAP (note firewalls are included in the path, but not shown).

8.1.13 Demarc 13

This demarcation point is between the NG9-1-1 PSAP and the location server (e.g., LIS or LRF) in an IP-based originating network and/or the ADR in an IP-based originating network. The demarcation is at NG9-1-1 PSAP (note firewalls are included in the path, but not shown).

8.2 Minimum Demarcation Points for the Typical NG9-1-1 Configuration

Figure 8 illustrates all of the possible demarcation points in an NG9-1-1 configuration that does not include LSRGs. In configurations being deployed today it is typical for the gateway functions (LNG and LPG) to be the responsibility of the NG9-1-1 Service Provider. In that case the minimum number of demarcation points required to evaluate reporting criteria are shown below.

- Demarc Point 1
- Demarc Point 2
- Demarc Point 3 (only for ingress IP)
- Demarc Point 5
- Demarc Point 8
- Demarc Point 9
- Demarc Point 10
- Demarc Point 11
- Demarc Point 12
- Demarc Point 13

9 Transitional Architecture Involving Legacy Selective Router Gateway

As described in *Section 5.2.2*, the LSRG supports the delivery of emergency calls that originate in networks that are served by legacy SRs and are destined for PSAPs that are served by NG Emergency Services Networks, as well as the delivery of emergency calls routed via an NG Emergency Services Network to legacy PSAPs that are served by legacy SRs. The LSRG also facilitates transfers of calls between PSAPs that are served by legacy SRs and PSAPs that are served by NG Emergency Services Networks. An LSRG may reside on either the ingress or the egress side of an NG Emergency Services Network. While an LSRG is generally assumed to be operated by the same entity as operates the SR, there are demarcation points beyond those described in *Section 0* that are associated with transitional architectures that include LSRGs. These demarcation points influence the visibility that originating network providers and NG9-1-1SSPs have into potential failures that may occur with respect to emergency call delivery, location information delivery, and callback information delivery, when a transitional architecture involving LSRGs is used.

9.1 Ingress LSRG

In a transitional architecture where originating networks are served by legacy SRs and emergency calls are routed to NG Emergency Services Networks via an ingress LSRG, the amount of visibility that the originating network provider and NG9-1-1SSP have into downstream elements/networks will be similar to architectures involving an LNG, where the LNG is operated by the NG9-1-1SSP. A transitional architecture involving an ingress LSRG, with the associated demarcation points, is depicted below.

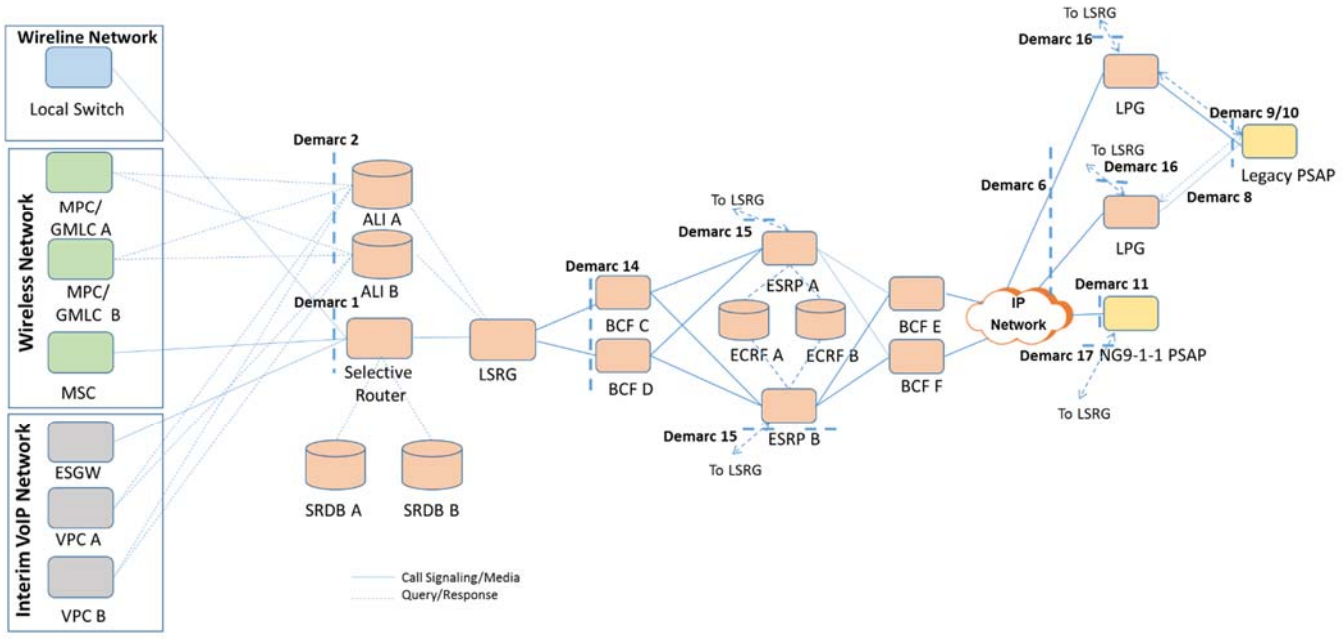


Figure 9 - Transitional Functional Architecture with Ingress Legacy Selective Router Gateway

9.1.1 Demarcation Points for Ingress LSRG

Figure 9 illustrates demarcation points between network providers that denote where responsibility lies for managing and reporting failures. Only the demarcation points that are unique to a transitional architecture that includes an ingress LSRG are defined below. See *Section 0* for descriptions of the other demarcation points included in this figure.

9.1.1.1 Demarc 14

This demarcation point is between the ingress LSRG and the NG Emergency Services Network Border Control Function (BCF) and supports call delivery to the NG Emergency Services Network. The demarcation point is at the ingress to the Emergency Services Network BCF.

9.1.1.2 Demarc 15

If location and/or Additional Data is sent by the LSRG with the emergency call "by-reference", the ESRP in the NG Emergency Services Network will send a dereference request to the LSRG to obtain the location/Additional Data "by-value". The demarcation point that supports this dereferencing is at the ESRP (note firewalls are included in the path, but not shown).

9.1.1.3 Demarc 16

This demarcation point applies if the architecture involves an LPG as well as an ingress LSRG. This demarcation point is used by the LPG to request the dereferencing of location and/or Additional Data if the location and/or Additional Data were provided by the ingress LSRG "by-reference". The demarcation point is at the LPG (note firewalls are included in the path, but not shown).

9.1.1.4 Demarc 17

If the location and/or the Additional Data is sent by the ingress LSRG "by-reference", the NG9-1-1 PSAP will send a dereference request to the LSRG to obtain the location and/or Additional Data "by-value". The demarcation point is at NG9-1-1 PSAP (note firewalls are included in the path, but not shown).

9.2 Egress LSRG

In a transitional architecture where an emergency call routed via an NG Emergency Services Network is delivered via an egress LSRG to a PSAP that is served by a legacy SR, the amount of visibility that the originating network provider and NG9-1-1SSP have into downstream elements/networks will be similar to architectures involving an LPG, where the LPG is operated by an entity other than the NG9-1-1SSP. A transitional architecture involving an egress LSRG, with the associated demarcation points, is depicted below.

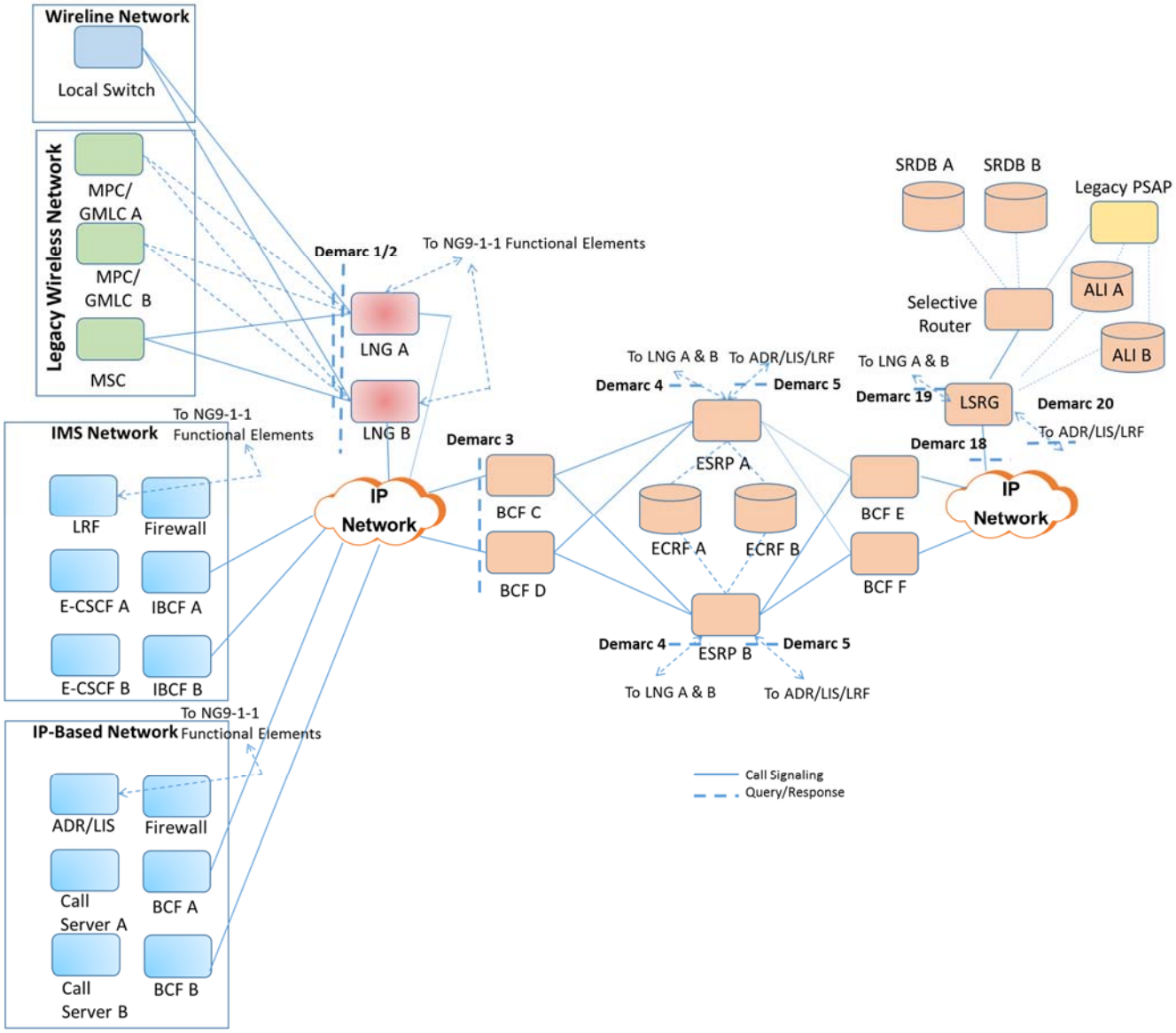


Figure 10 – Transitional Functional Architecture with Egress Legacy Selective Router Gateway

9.2.1 Demarcation Points for Egress LSRG

Figure 10 illustrates demarcation points between network providers that denote where responsibility lies for managing and reporting failures. Only the demarcation points that are unique to a transitional architecture involving an egress LSRG are defined below. See *Section 0* for descriptions of the other demarcation points included in this figure.

9.2.1.1 Demarc 18

This demarcation point is between the NG Emergency Services Network Border Control Function and the egress LSRG to support call delivery to a PSAP that is served by a legacy SR.

The demarcation point is at the ingress side of the LSRG (note that the LSRG may have an additional BCF, not shown).

9.2.1.2 Demarc 19

If location and/or Additional Data is generated by an LNG and delivered to the egress LSRG with the emergency call "by-reference", the egress LSRG will send a dereference request to the LNG to obtain the location/additional data "by-value". The demarcation point that supports this dereferencing is at the egress LSRG (note firewalls are included in the path, but not shown).

9.2.1.3 Demarc 20

This demarcation point is between the egress LSRG and the location server (e.g., LIS or LRF) and/or the ADR in an IP-based originating network. This demarcation point applies if the emergency call originates in an IP-based originating network and location and/or Additional Data is delivered to the egress LSRG "by-reference". This demarcation point is used by the egress LSRG to request the dereferencing of location and/or Additional Data. The demarcation point is at the egress LSRG (note firewalls are included in the path, but not shown).

10 Architectural Analysis

This section analyzes the transitional and end-state NG9-1-1 architectures described above from the perspective of call delivery failures, location delivery failures and callback information delivery failures, to identify which failures can be identified by various stakeholder roles. As discussed in *Section* 3.3.1, while the focus of the analysis is call delivery, location delivery, and callback information delivery failures, the analysis also considers failures related to the delivery of additional non-location data, such as class of service information and Service Provider contact information, that is typically delivered to PSAPs from ALI systems today. In this sense, the analysis examines transitional and end-state-NG9-1-1 architectures in terms of the call delivery failure and ANI/ALI delivery failure metrics applied to E9-1-1 architectures to determine the impact of NG9-1-1 on the ability of the different NG9-1-1 stakeholders to detect potentially service-affecting failures.

While not explicitly depicted in the figures in *Sections 8 and 9*, this analysis assumes that the transitional and end-state architectures described in this document deploy redundancy to improve the overall reliability of the architectures. As mentioned previously in this Report, the demarcation points are at the boundaries between the Emergency Services Network and other partner networks with which they interconnect. It is assumed in this Report that all network elements and transport facilities are deployed with redundancy. Network redundancy is primarily implemented in Emergency Services Network infrastructure to provide an alternate path for network communications. It serves as a mechanism for quickly swapping network operations onto redundant infrastructure in the event of an error within a network element or transmission path. Typically, network redundancy is achieved through the addition of alternate network paths, which are implemented through redundant standby network elements, routers and switches. When the primary path is unavailable, the alternate path can be instantly deployed to ensure continuity of network services. As such the switching to a backup configuration, in general, does not cause service degradation.

10.1 NG9-1-1 Failure Considerations – All IP End-State

In an end state (all IP) NG9-1-1 environment, the originating network has limited visibility into the Emergency Services Network. The visibility exists up to Demarc Point 3 for call delivery and for location/Additional Data delivery where that information is signaled forward "by value". For dereferencing of location information and Additional Data that was signaled forward by the originating network "by reference", the originating network has visibility up to Demarc Point 5 for dereference requests sent by an ESRP, and up to Demarc Point 13 for dereference requests sent by an i3 PSAP. The originating network does not have visibility into the PSAP for call delivery or for information (i.e., location or Additional Data) delivery where that information was signaled by the originating network "by value". The NG Emergency Services Network has visibility directly into the PSAP (i.e., via Demarc Point 11) for call delivery, including the delivery of location and Additional Data ("by reference" or "by value"), as well as callback information, via SIP based call setup signaling, but it is not aware of what data may be exchanged between the PSAP and the originating network (i.e., via Demarc Point 13). This section analyzes where failures in call and data delivery may be detected in an NG9-1-1 environment.

10.1.1 Call Delivery Failures

10.1.1.1 Failures Detected by Originating Network

An IP-based originating network will be expected to monitor for transport alarms associated with IP connections to the NG Emergency Services Network. An IP originating network may also detect emergency call delivery failures via call failure indications/messages received via signaling. Based on the signaling indications received, the originating network may be able to determine the nature and location of the failure.

10.1.1.2 Failures Detected by NG9-1-1 System Service Provider

An NG9-1-1 System Service Provider (NG9-1-1SSP) will be able to detect when IP connectivity to the PSAP, or IP connectivity between the first routing element in the NG Emergency Services Network and other downstream network elements, is unavailable, resulting in alternate routing of the emergency call or PSAP isolation. The NG9-1-1SSP will be responsible for monitoring IP connections for transport alarms. Where appropriate, heartbeats may be used to verify the availability of network facilities. NG9-1-1SSPs should provide the means for capturing network traffic, generating alarms, and producing other metrics for monitoring and troubleshooting outages within NG Emergency Services Networks, as well as those impacting the ability of an NG Emergency Services Network to deliver calls to the target PSAP.

10.1.2 Location Delivery Failures

10.1.2.1 Failures Detected by Originating Network Providers

IP-based originating network providers will have the ability to determine whether or not location information is included in the outgoing SIP signaling sent to an NG Emergency Services Network. If the originating network provider fails to include location information (by-value or

by-reference) in outgoing SIP signaling to an NG Emergency Services Network, it can conclude that location information was not delivered to the PSAP.

If the IP-based originating network provider is serving fixed customers, and location information is included in outgoing SIP signaling sent to the NG Emergency Services Network, the location information delivered to the NG Emergency Services Network (i.e., via Demarc Point 3) with the call will typically be in the form of location-by-value. An originating network provider that delivers location-by-value to an NG Emergency Services Network will not be able to determine whether or not that location information is subsequently delivered to the PSAP.

IP-based originating network providers that serve mobile callers will be responsible for providing caller location dynamically per call. To support the dynamic delivery of location information associated with emergency calls originated by mobile users, the IP-based originating network will provide location-by-reference in the SIP signaling delivered to the NG Emergency Services Network (via Demarc Point 3). The originating network provider must also support location dereference requests from routing elements in the NG Emergency Services Network (via Demarc Point 5) as well as NG PSAPs (via Demarc Point 13). If an IP-based originating network receives a dereference request from an NG PSAP, it can conclude that the location-by-reference that it signaled to the NG Emergency Services Network was successfully delivered to the NG PSAP. In addition, the IP-based originating network will be able to detect any failures to provide location-by-value in response to location dereference requests from NG Emergency Services Network elements or NG PSAPs.

10.1.2.2 Failures Detected by NG9-1-1 System Service Providers

Routing elements in an NG Emergency Services Network will be able to detect failures in the delivery of location information to the NG Emergency Services Network. If the IP-based originating network fails to provide location information to the NG Emergency Services Network in the SIP signaling associated with an emergency call, the NG Emergency Services Network will perform default routing of the emergency call. The NG Emergency Services Network will be able to determine whether location information received from the originating network ("by-value" or "by-reference") with the call is successfully delivered to the NG PSAP.

When a routing element in an NG Emergency Services Network receives location-by-reference, it will launch a dereference request to an element in the IP originating network. The NG9-1-1SSP will be able to detect failures in the dereference process if a routing element in the NG Emergency Services Network does not receive a location-by-value in response to the location dereference request.

10.1.3 Callback Information Delivery Failures

10.1.3.1 Failures Detected by Originating Network Providers

IP-based originating network providers have the ability to determine whether outgoing signaling delivered to an NG Emergency Services Network (via Demarc Point 3) includes callback information, but they will not be able to detect whether the callback information was successfully delivered to the PSAP.

10.1.3.2 Failures Detected by NG9-1-1 System Service Providers

NG9-1-1SSPs will be able to determine whether callback information was received in incoming signaling from an IP originating network, and will also be able detect whether callback information was successfully delivered to the PSAP (i.e., via Demarc Point 11).

10.2 NG9-1-1 Failure Considerations – Interworking Architecture Involving Legacy Network Gateway

In an interworking architecture where a legacy originating network interfaces to an LNG that resides between the originating network and the NG Emergency Services Network, the amount of visibility that the originating network has into downstream elements/networks will depend on what entity has responsibility for the LNG and where the demarcation points are drawn. If the LNG is operated by the NG9-1-1 System Service Provider, then the originating network will only have visibility into what is delivered to the LNG to support call delivery (i.e., via Demarc Point 1) and location/Additional Data delivery (i.e., via Demarc Point 2). Call delivery from the originating network to the LNG will be via SS7 or MF trunk groups, with location delivered in the form of a 10-digit location key (i.e., calling number/ANI, ESRK, ESRD). If the LNG is operated by the originating network provider, then the originating network will also have visibility into the Emergency Services Network for call delivery (i.e., via Demarc Point 3) and for location/Additional Data delivery (i.e., via Demarc Point 4). Using this type of arrangement, call delivery from the LNG to the Emergency Services Network will be via SIP, with location and Additional Data delivered either “by value” or “by reference”.

If the NG9-1-1 System Service Provider operates the LNG, the originating network will have visibility into the LNG (i.e., via Demarc Point 2) to support location queries (using legacy protocols such as E2 or MLP) generated by the LNG to MPCs/GMLCs to obtain location and other information associated with legacy wireless emergency originations. If the originating network provider operates the LNG, the originating network provider will have visibility into the ESRP in the NG Emergency Services Network (i.e., via Demarc Point 4) and the i3 PSAP (i.e., via Demarc Point 13) for dereferencing of location information and Additional Data that was signaled forward by the LNG “by-reference”. Regardless of which network provider is responsible for operating the LNG, the originating network will not have visibility into the PSAP for call delivery or for information (i.e., location or Additional Data) delivery where that information was signaled by the originating network “by-value”. The entity that is responsible for operating the LNG will however have visibility into whether location or Additional Data was successfully delivered to the i3 PSAP “by reference” if the LNG receives a dereference request from the i3 PSAP (i.e., via Demarc 13).

The NG Emergency Services Network will have visibility directly into the PSAP (i.e., via Demarcation Point 11) for call delivery, including the delivery of location and Additional Data (“by-reference” or “by value”), as well as callback information, via SIP-based call setup signaling. This section analyzes where failures in call and data delivery may be detected in an interworking environment where the service architecture includes an LNG.

10.2.1 Call Delivery Failures

10.2.1.1 Failures Detected by Originating Network Providers

A legacy originating network will be expected to monitor for transport alarms associated with SS7 or MF trunk groups to the LNG. If the originating network provider is also responsible for operating the LNG, the originating network will also be expected to monitor for transport alarms associated with IP connections to the NG Emergency Services Network. A legacy originating network may also detect emergency call delivery failures via call failure indications/messages received from the LNG via MF/SS7 signaling. Based on the signaling indications received, the originating network may be able to determine the nature and location of the failure. If the originating network provider is also responsible for operating the LNG, the originating network provider will also detect call delivery failure indications received by the LNG via SIP signaling.

10.2.1.2 Failures Detected by NG9-1-1 System Service Providers

As for the all-IP end-state configuration, an NG9-1-1SSP will be able to detect when IP connectivity to the PSAP, or IP connectivity between the first routing element in the NG Emergency Services Network and other downstream network elements, is unavailable, resulting in alternate routing of the emergency call or PSAP isolation. The NG9-1-1SSP will be responsible for monitoring IP connections for transport and for capturing network traffic, generating alarms and producing other metrics for monitoring and troubleshooting outages within NG Emergency Services Networks, as well as those impacting the ability of an NG Emergency Services Network to deliver calls to the target PSAP.

If the NG9-1-1SSP is also responsible for operating the LNG, the NG9-1-1SSP will also be able to detect any errors in the SS7/MF call delivery signaling from the originating network.

10.2.2 Location Delivery Failures

10.2.2.1 Failures Detected by Originating Network Providers

Legacy originating network providers will have the ability to determine whether or not a calling number/ANI and/or a pANI (e.g., ESRK, ESRD) is included in the outgoing MF or SS7 signaling sent to an LNG (i.e., via Demarc Point 1) with an emergency call. If the originating network provider fails to include a calling number/ANI and/or a pANI in outgoing SS7 or MF signaling to LNG, it can determine that location information was not delivered to the PSAP.

If the originating network provider is also responsible for operating the LNG, the originating Service Provider will have the ability to determine whether or not location information is included in the outgoing SIP signaling sent by the LNG to an NG Emergency Services Network (i.e., via Demarc Point 3). If the originating network provider/LNG operator fails to include location information (by value or by reference) in outgoing SIP signaling to an NG Emergency Services Network, it can determine that location information was not delivered to the PSAP.

If the originating network provider is serving fixed customers, and location information is included in outgoing SIP signaling sent by the originating network provider/LNG operator to the NG Emergency Services Network, the location information delivered to the NG Emergency Services Network (i.e., via Demarc Point 3) with the call will typically be in the form of location by value. An LNG that delivers location by value to an NG Emergency Services Network will

not be able to determine whether or not that location information is subsequently delivered to the PSAP by the NG Emergency Services Network.

Legacy wireless originating network providers that include a pANI in the SS7 or MF signaling sent to the LNG will be responsible for providing caller location when queried by an LNG (i.e., via Demarc Point 2) using the E2 protocol or MLP. If the legacy wireless originating network receives a request for updated caller location from an LNG, it can assume that the NG PSAP/LPG received a location by reference associated with the emergency call. The legacy wireless originating network provider will be able to determine whether the location request from the LNG was processed successfully, but unless they also operate the LNG, they will not know whether the location information was successfully returned to the NG PSAP/LPG. If the legacy wireless originating network provider operates the LNG, it will be able to determine whether location information (by reference) was successfully provided by the LNG to the NG Emergency Services Network with the call using SIP signaling (i.e., via Demarc Point 3). An originating network provider that operates an LNG must also support location dereference requests from routing elements in the NG Emergency Services Network (via Demarc Point 4) as well as NG PSAPs (via Demarc Point 13). If an LNG receives a dereference request from an NG PSAP, it can conclude that that the location by reference that it signaled to the NG Emergency Services Network was successfully delivered to the NG PSAP. In addition, the LNG will be able to detect any failures to provide location by value in response to location dereference requests from NG Emergency Services Network elements or NG PSAPs.

10.2.2.2 Failures Detected by NG9-1-1 System Service Providers

Routing elements in an NG Emergency Services Network will be able to detect failures in the delivery of location information to the NG Emergency Services Network. If the LNG fails to provide location information to the NG Emergency Services Network in the SIP signaling associated with an emergency call, the NG Emergency Services Network will perform default routing of the emergency call. The NG9-1-1SSP will be able to determine whether location information received from the LNG ("by-value" or "by-reference") with the call is successfully delivered to the NG PSAP (i.e., via Demarc 11) or the LPG (i.e., via Demarc Point 6).

When a routing element in an NG Emergency Services Network receives location-by-reference from an LNG, it will launch a dereference request back to the LNG to obtain the routing location. The NG9-1-1SSP will be able to detect failures in the dereference process if a routing element in the NG Emergency Services Network does not receive a location-by-value in response to the location dereference request.

If the NG9-1-1SSP is also responsible for operating the LNG, it will also have visibility into whether a location query initiated toward a legacy wireless network resulted in the successful return of location information, and whether location dereference requests from routing elements in the NG Emergency Services Network, NG PSAPs, or LPGs were successfully processed by the LNG.

10.2.3 Callback Information Delivery Failures

10.2.3.1 Failures Detected by Originating Network Providers

Legacy wireline originating network providers and legacy wireless originating network providers that use the NCAS method have the ability to determine whether outgoing MF or SS7 signaling delivered to an LNG (i.e., via Demarc 1) includes an MF ANI or SS7 Calling Party Number, but they will not be able to detect whether the callback information was successfully delivered to the PSAP. Legacy wireless originating network providers that use the WCM approach for emergency calls will be able to determine whether callback information is returned in response to an E2 or MLP request from an LNG (i.e., via Demarc Point 2).

If the legacy originating network provider also operates the LNG, it will be able to determine whether the SIP signaling delivered to the Emergency Services Network (via Demarc Point 3) includes callback information, but they will not be able to detect whether the callback information was successfully delivered to the PSAP.

10.2.3.2 Failures Detected by NG9-1-1 System Service Providers

NG9-1-1SSPs will be able to determine whether callback information was received in incoming signaling from an LNG, and will also be able detect whether callback information was successfully delivered to an NG PSAP (i.e., via Demarc Point 11) or an LPG (i.e., via Demarc Point 6).

If the NG9-1-1SSP is also responsible for operating the LNG, it will also have visibility into whether callback information was delivered in call setup signaling (i.e., in the form of an MF ANI or SS7 Calling Party Number via Demarc Point 1), or whether it was obtained as part of the location response from a legacy wireless originating network (i.e., via Demarc Point 2).

10.3 NG9-1-1 Failure Considerations - Interworking Architecture Involving Legacy PSAP Gateway

In an interworking architecture where a legacy PSAP interfaces to an LPG that resides between the legacy PSAP and the NG Emergency Services Network, the amount of visibility that the NG Emergency Services Network has into the PSAP will depend on what entity has responsibility for the LPG and where the demarcation points are drawn. If the LPG is operated by the PSAP (or a third party other than the NG Emergency Services Network provider), then the NG Emergency Services Network will only have visibility into what is delivered to the LPG to support call delivery (i.e., via Demarc Point 6), including the delivery of location and Additional Data (“by-reference” or “by value”), as well as callback information, via SIP-based call setup signaling. It will not have visibility into what the LPG delivers to the PSAP with the call. The NG Emergency Services Network will also not be aware of what data may be exchanged between the LPG (on behalf of the PSAP) and the originating network (i.e., via Demarc Point 8), or between the LPG and the LNG (i.e., via Demarc Point 7).

If the LPG is operated by the provider of the NG Emergency Services Network (i.e., the NG9-1-1SSP), then in addition to having an awareness of the status of the IP connection between the NG Emergency Services Network and the LPG, and what information (e.g., callback information, location information “by-value” or “by-reference”, Additional Data “by value” or “by reference”) is delivered via SIP signaling to the LPG, the NG Emergency Services Network

will have visibility directly into the PSAP (i.e., via Demarc Point 9) for call delivery. In this case, the NG9-1-1SSP will be aware of the status of the MF trunk group to the PSAP as well as what information is conveyed via Traditional MF or E-MF signaling between the LPG and the legacy PSAP. If the NG9-1-1SSP operates the LPG, then it will also have visibility into the delivery of location information and other additional data to the PSAP using legacy ALI query/response protocols (i.e., via Demarc Point 10). It will also be aware of whether or not dereference requests launched by the LPG toward the originating network (i.e., via Demarc Point 8) or toward an LNG (i.e., via Demarc Point 7) are successful in obtaining location information or Additional Data.

This section analyzes where failures in call and data delivery may be detected in an interworking environment where the service architecture includes an LPG.

10.3.1 Call Delivery Failures

10.3.1.1 Failures Detected by Originating Network

The ability for an IP-based originating network to detect call delivery failures in an architecture where emergency calls are delivered to legacy PSAPs via an LPG will be the same as described in *Section 10.1.1.1*. The only difference will be that the SIP-based call failure indications/messages will come from the LPG rather than from an NG PSAP. Likewise, the ability for a legacy originating network to detect call delivery failures in an architecture where emergency calls are delivered to legacy PSAPs via an LPG will be the same as described in *Section 10.2.1.1*, except that if the originating network provider is also the LNG operator, the originating network provider will receive SIP-based call delivery failure indications from the LPG rather than from an NG PSAP.

10.3.1.2 Failures Detected by NG9-1-1 System Service Providers

An NG9-1-1SSP will be able to detect when IP connectivity to the LPG is unavailable, the NG9-1-1SSP will be responsible for monitoring these IP connections for transport alarms. If the NG9-1-1SSP is also responsible for operating the LPG, then it will be able to detect when the MF (emergency message) trunks to the PSAP are unavailable, preventing calls from being delivered to the target legacy PSAP.

10.3.2 Location Delivery Failures

10.3.2.1 Failures Detected by Originating Network

The ability for an IP-based originating network to detect location delivery failures in an architecture where emergency calls are delivered to legacy PSAPs via an LPG will be the same as described in *Section 10.1.2.1*, with the following clarification. The originating network provider must also support location dereference requests from LPGs (via Demarc Point 8), as well as routing elements in the NG Emergency Services Network (via Demarc Point 5) and NG PSAPs (via Demarc Point 13). If an IP-based originating network receives a dereference request from an LPG, it can conclude that the location-by-reference that it signaled to the NG Emergency Services Network was successfully delivered to the LPG, but it will not have visibility into whether or not location is successfully delivered to the legacy PSAP. In addition,

the IP-based originating network will be able to detect any failures to provide location-by-value in response to location dereference requests from LPGs.

The ability for a legacy originating network to detect location delivery failures in an architecture where emergency calls are delivered to legacy PSAPs via an LPG will be the same as described in *Section 10.2.2.1*, with the following clarification. An originating network provider that operates an LNG must support location dereference requests from LPGs (via Demarc Point 7), as well as from routing elements in the NG Emergency Services Network (via Demarc Point 4) and NG PSAPs (via Demarc Point 13). If an LNG receives a dereference request from an LPG, it can conclude that the location-by-reference that it signaled to the NG Emergency Services Network was successfully delivered to the LPG, but it will have no visibility into whether or not location information is successfully delivered to the legacy PSAP. The LNG will also be able to detect any failures to provide location-by-value in response to location dereference requests from LPGs.

10.3.2.2 Failures Detected by NG9-1-1 System Service Provider

The ability for an NG9-1-1SSP to detect location delivery failures in an architecture where emergency calls are delivered to legacy PSAPs via an LPG will be the same as described in *Sections 10.1.2.2 and 10.2.2.2*, with the following clarifications. The NG9-1-1SSP will be able to determine whether location information received from the IP originating network or LNG ("by-value" or "by-reference") with the call is successfully delivered to the LPG (i.e., via Demarc Point 6), but will not be able to determine whether location information was successfully delivered to the legacy PSAP unless the NG9-1-1SSP also operates the LPG.

If the NG9-1-1SSP is also responsible for operating the LPG, it will have visibility into whether a location dereference request initiated toward an originating network/LNG resulted in the successful return of location information to the LPG, and whether location information was successfully delivered to the legacy PSAP.

10.3.3 Callback Information Delivery Failures

10.3.3.1 Failures Detected by Originating Network Providers

IP-based originating network providers will have the ability to determine whether outgoing signaling delivered to an NG Emergency Services Network (via Demarc Point 3) includes callback information, but they will not be able to detect whether the callback information was successfully delivered to the LPG or the PSAP.

The ability for a legacy originating network to detect failures in the delivery of callback information in an architecture where emergency calls are delivered to legacy PSAPs via an LPG will be the same as described in *Section 10.2.3.1*, with the following clarification. Legacy wireline originating network providers and legacy wireless originating network providers that use the NCAS method will be able to determine whether outgoing MF or SS7 signaling delivered to an LNG (i.e., via Demarc 1) includes an MF ANI or SS7 Calling Party Number, but they will not be able to detect whether the callback information was successfully delivered to the LPG or to the PSAP. If the legacy originating network provider also operates the LNG, it will be able to determine whether the SIP signaling delivered to the Emergency Services Network (via

Demarc Point 3) includes callback information, but they will not be able to detect whether the callback information was successfully delivered to the LPG or to the PSAP.

10.3.3.2 Failures Detected by NG9-1-1 System Service Providers

NG9-1-1SSPs will be able to determine whether callback information was received in incoming signaling from an IP originating network or LNG, and will also be able detect whether callback information was successfully delivered to an LPG (i.e., via Demarc Point 6), but they will not be able to detect whether callback information was successfully delivered to the PSAP, unless the NG9-1-1SSP also operates the LPG. If the NG9-1-1SSP is also responsible for operating the LPG, it will have visibility into whether callback information was successfully delivered to the legacy PSAP.

10.4 NG9-1-1 Failure Considerations - Transitional Architecture Involving LSRG

10.4.1 Ingress Legacy Selective Router Gateway

10.4.1.1 Call Delivery Failures

10.4.1.1.1 Failures Detected by Originating Network Providers

As in E9-1-1 architectures today, a legacy originating network will be expected to monitor for transport alarms associated with SS7 or MF trunk groups to the SR. A legacy originating network may also detect emergency call delivery failures via call failure indications/messages received from the SR via MF/SS7 signaling. Based on the signaling indications received (e.g., the Cause Indicator parameter value in an SS7 Release message), the originating network may be able to determine the nature and location of the failure.

10.4.1.1.2 Failures Detected by E9-1-1 System Service Providers

Since the E9-1-1SSP is also expected to be responsible for operating the ingress LSRG, the E9-1-1SSP will also be expected to monitor for transport alarms associated with IP connections to the NG Emergency Services Network. The E9-1-1SSP will also be able to detect call delivery failure indications received by the LSRG via SIP signaling from the NG Emergency Services Network.

10.4.1.1.3 Failures Detected by NG9-1-1 System Service Providers

As for the all-IP end-state configuration and interworking architectures involving LNGs, an NG9-1-1SSP will be able to detect when IP connectivity to the PSAP, or IP connectivity between the first routing element in the NG Emergency Services Network and other downstream network elements, is unavailable, resulting in alternate routing of the emergency call or PSAP isolation. The NG9-1-1SSP will be responsible for monitoring IP connections for transport alarms associated with IP connections from ingress LSRGs and between elements within the NG Emergency Services Network. The NG9-1-1SSP will be responsible for capturing network traffic, generating alarms and producing other metrics for monitoring and troubleshooting

outages within NG Emergency Services Networks, as well as those impacting the ability of an NG Emergency Services Network to deliver calls to the target PSAP.

10.4.1.2 Location Delivery Failures

10.4.1.2.1 Failures Detected by Originating Network Providers

As for interworking architectures involving LNGs, legacy originating network providers will have the ability to determine whether or not a calling number/ANI and/or a pANI (e.g., ESRK, ESRD) is included in the outgoing MF or SS7 signaling sent to an SR (i.e., via Demarc Point 1) with an emergency call. If the originating network provider fails to include a calling number/ANI and/or a pANI in outgoing SS7 or MF signaling to the SR, it can conclude that location information will not be delivered to the PSAP.

Legacy wireless originating network providers will be responsible for providing caller location when queried by a legacy ALI system (i.e., via Demarc Point 2) using the E2 protocol or MLP. If the legacy wireless originating network receives a request for updated caller location from a legacy ALI system, it can assume that the NG PSAP/LPG received a location-by-reference associated with the emergency call, and that the ingress LSRG received a dereference request from the NG PSAP/LPG (see below for further details). The legacy wireless originating network provider will be able to determine whether the location request from the legacy ALI system was processed successfully, but they will not know whether the location information was successfully returned to the NG PSAP/LPG.

10.4.1.2.2 Failures Detected by E9-1-1 System Service Providers

Since the E9-1-1SSP is assumed to also be responsible for operating the ingress LSRG, the E9-1-1SSP will have the ability to determine whether or not location information is included in the outgoing SIP signaling sent by the LSRG to an NG Emergency Services Network (i.e., via Demarc Point 14). If the E9-1-1SSP/LSRG operator fails to include location information (by-value or by-reference) in outgoing SIP signaling to an NG Emergency Services Network, it can conclude that location information was not delivered to the PSAP.

When the E9-1-1SSP receives emergency calls from a legacy wireline originating network provider, the location information delivered to the NG Emergency Services Network (i.e., via Demarc Point 14) with the call will typically be in the form of location-by-value. An LSRG that delivers location-by-value to an NG Emergency Services Network will not be able to determine whether or not that location information is subsequently delivered to the PSAP by the NG Emergency Services Network.

When the E9-1-1SSP receives an incoming emergency call from a legacy wireless originating network, the E9-1-1SSP will be able to determine whether location information (by-reference) was successfully provided by the LSRG to the NG Emergency Services Network with the call using SIP signaling (i.e., via Demarc Point 14). The E9-1-1SSP must also support location dereference requests to the ingress LSRG from routing elements in the NG Emergency Services Network (via Demarc Point 15) as well as NG PSAPs (via Demarc Point 17) and LPGs (via Demark Point 16). If an LSRG receives a dereference request from an NG PSAP, it can conclude that that the location-by-reference that it signaled to the NG Emergency Services

Network was successfully delivered to the NG PSAP. The E9-1-1SSP will also be able detect any failures by the LSRG to provide location-by-value in response to location dereference requests from NG Emergency Services Network elements, NG PSAPs, or LPGs.

10.4.1.2.3 Failures Detected by NG9-1-1 System Service Providers

Routing elements in an NG Emergency Services Network will be able to detect failures in the delivery of location information to the NG Emergency Services Network. If an ingress LSRG fails to provide location information to the NG Emergency Services Network in the SIP signaling associated with an emergency call, the NG Emergency Services Network will perform default routing of the emergency call. The NG9-1-1SSP will be able to determine whether location information received from an ingress LSRG ("by-value" or "by-reference") with the call is successfully delivered to the NG PSAP (i.e., via Demarc 11) or the LPG (i.e., via Demarc Point 6).

When a routing element in an NG Emergency Services Network receives location-by-reference from an ingress LSRG, it will launch a dereference request back to the LSRG to obtain the routing location. The NG9-1-1SSP will be able to detect failures in the dereference process if a routing element in the NG Emergency Services Network does not receive a location-by-value in response to the location dereference request.

The NG9-1-1SSP will not have visibility into location dereference requests initiated by NG9-1-1 PSAPs or LPGs toward ingress LSRGs.

10.4.1.3 Callback Information Delivery Failures

10.4.1.3.1 Failures Detected by Originating Network Providers

Legacy wireline originating network providers and legacy wireless originating network providers that use the NCAS method have the ability to determine whether outgoing MF or SS7 signaling delivered to an SR (i.e., via Demarc 1) includes an MF ANI or SS7 Calling Party Number, but they will not be able to detect whether the callback information was successfully delivered to the PSAP.

Legacy wireless originating network providers that use the WCM approach for emergency calls will be able to determine whether callback information is returned in response to an E2 or MLP request from a legacy ALI (i.e., via Demarc Point 2). However, the originating network provider will not have visibility into the availability of that information to any other network element or PSAP.

10.4.1.3.2 Failures Detected by E9-1-1 System Service Providers

The E9-1-1SSP (which is assumed to also be responsible for operating the ingress LSRG) will have the ability to determine whether or not callback information was received from the originating network (i.e., via Demarc Point 2), in call setup signaling, and whether it is included in the outgoing SIP signaling sent by the LSRG to an NG Emergency Services Network (i.e., via Demarc Point 14) to establish the emergency call. An LSRG that delivers callback information to an NG Emergency Services Network will not be able to determine whether or not that

callback information is subsequently delivered to the PSAP by the NG Emergency Services Network.

An E9-1-1SSP will also be able to recognize when an LSRG queries an ALI system for location/callback information, and the ALI system in turn queries the legacy wireless originating network for location/callback information using the E2 protocol or MLP. The E9-1-1SSP will be able to determine whether callback information was successfully obtained by the ALI system from the legacy wireless originating network (i.e., via Demarc Point 2), and was successfully delivered to the LSRG. As described above, the E9-1-1SSP will be able to determine whether callback information was successfully delivered to an NG Emergency Services Network in outgoing SIP signaling, but will not be able to determine whether callback information was successfully delivered to the PSAP.

10.4.1.3.3 Failures Detected by NG9-1-1 System Service Providers

NG9-1-1SSPs will be able to determine whether callback information was received in incoming signaling from an ingress LSRG (i.e., via Demarc Point 14), and will also be able detect whether callback information was successfully delivered to an NG PSAP (i.e., via Demarc Point 11) or an LPG (i.e., via Demarc Point 6) in call setup signaling.

As described in *Section 10.3.3.2*, an NG9-1-1SSP will not be able to detect whether callback information was successfully delivered to a legacy PSAP via an LPG, unless the NG9-1-1SSP also operates the LPG. If the NG9-1-1SSP is also responsible for operating the LPG, it will have visibility into whether callback information was successfully delivered to the legacy PSAP.

10.4.2 Egress Legacy Selective Router Gateway

10.4.2.1 Call Delivery Failures

10.4.2.1.1 Failures Detected by Originating Network Providers

The ability for an IP-based originating network to detect call delivery failures in an architecture where emergency calls are delivered to legacy PSAPs via SRs that are connected to NG Emergency Services Networks via egress LSRGs is the same as described in *Section 10.1.1.1* , with the exception that the SIP-based call failure indications/messages will come from the egress LSRG rather than from an NG PSAP.

The ability for a legacy originating network to detect call delivery failures in an architecture where emergency calls are delivered to legacy PSAPs via SRs that are interconnected to egress LSRGs is the same as described in *Section 10.2.1.1*, except that if the originating network provider is also the LNG operator, the originating network provider will receive SIP-based call delivery failure indications (i.e., at the LNG) from the egress LSRG rather than from an NG PSAP.

10.4.2.1.2 Failures Detected by NG9-1-1 System Service Providers

An NG9-1-1SSP will be able to detect when IP connectivity to the egress LSRG (i.e., via Demarc Point 18) is unavailable. The NG9-1-1SSP will be responsible for monitoring these IP connections for transport alarms. The NG9-1-1SSP will not be able to detect when the MF

(emergency message) trunks to the PSAP are unavailable. SIP-based call delivery failure indications generated by the egress LSRG in response to SS7 Release messages with certain Cause Indicator parameter values will be passed to the NG Emergency Services Network. This will allow the NG9-1-1SSP to indirectly detect when there is a failure to deliver an emergency call to a legacy PSAP that is served by an SR.

10.4.2.1.3 Failures Detected by E9-1-1 System Service Providers

Since the E9-1-1SSP is also expected to be responsible for operating the egress LSRG, the E9-1-1SSP will be expected to monitor for transport alarms associated with IP connections from the NG Emergency Services Network.

An E9-1-1SSP will also be able to detect when SS7 connectivity from the egress LSRG, or MF connectivity to the PSAP, is unavailable, resulting in SR or PSAP isolation. The E9-1-1SSP will be responsible for capturing network traffic, generating alarms and producing other metrics for monitoring and troubleshooting outages within the legacy Emergency Services Network elements and the egress LSRG.

10.4.2.2 Location Delivery Failures

10.4.2.2.1 Failures Detected by Originating Network Providers

The ability for an IP-based originating network to detect location delivery failures in an architecture where emergency calls are delivered to legacy PSAPs via SRs that are connected to NG Emergency Services Networks via egress LSRGs will be the same as described in *Section 10.1.2.1* , with the following clarification. The originating network provider must also support location dereference requests from egress LSRGs (via Demarc Point 20). If an IP-based originating network receives a dereference request from an egress LSRG, it can conclude that the location-by-reference that it signaled to the NG Emergency Services Network was successfully delivered to the LSRG, but it will not have visibility into whether or not location is successfully delivered to the legacy PSAP. In addition, the IP-based originating network will be able to detect any failures to provide location-by-value in response to location dereference requests from LSRGs.

The ability for a legacy originating network to detect location delivery failures in an architecture where emergency calls are delivered to legacy PSAPs by SRs that are connected to NG Emergency Services Networks via egress LSRGs will be the same as described in *Section 10.2.2.1*, with the following clarification. An originating network provider that operates an LNG must support location dereference requests from egress LSRGs (via Demarc Point 19). If an LNG receives a dereference request from an LSRG, it can conclude that that the location-by-reference that it signaled to the NG Emergency Services Network was successfully delivered to the LSRG, but it will have no visibility into whether or not location information is successfully delivered to the legacy PSAP. The LNG will also be able to detect any failures to provide location-by-value in response to location dereference requests from LSRGs.

10.4.2.2.2 Failures Detected by NG9-1-1 System Service Providers

The ability for an NG9-1-1SSP to detect location delivery failures in an architecture where emergency calls are delivered to legacy PSAPs by SRs that are connected to NG Emergency

Services Networks via egress LSRGs will be the same as described in *Sections* 10.1.2.2 *and 10.2.2.2*, with the following clarifications. The NG9-1-1SSP will be able to determine whether location information received from the IP originating network or LNG ("by-value" or "by-reference") with the call is successfully delivered to the egress LSRG (i.e., via Demarc Point 18), but will not be able to determine whether location information was successfully delivered to the legacy PSAP.

10.4.2.2.3 Failures Detected by E9-1-1 System Service Providers

Since the E9-1-1SSP is assumed to also be responsible for operating the egress LSRG, the E9-1-1SSP will have the ability to determine whether or not location information was included in the incoming SIP signaling received by the egress LSRG from an NG Emergency Services Network (i.e., via Demarc Point 18). The E9-1-1SSP will also be able to determine whether a calling number and/or pANI (i.e., the location key generated by the egress LSRG) was received by the SR in incoming SS7 signaling from the egress LSRG, and the SR was able to successfully deliver that information to the target PSAP with the call. If the SR fails to receive a calling number/pANI in incoming signaling from the LSRG, it will include a substitute ANI string (e.g., 0-9-1-1-0000 or 000-9-1-1-0000) in the signaling to the PSAP. If an ANI failure condition is encountered by an SR, the E9-1-1SSP can also conclude that an ALI failure has occurred, since the calling number/pANI is the key to the location information for a call routed via an egress LSRG.

Since the E9-1-1SSP is also the LSRG provider, an E9-1-1SSP that is also an ALI provider will be responsible for steering location queries received by the ALI system from the PSAP to the egress LSRG. The E9-1-1SSP will be able to detect whether or not those queries result in the successful return of location information by the LSRG. An E9-1-1SSP that is also an ALI provider will also be able detect whether that location information was successfully returned by the ALI system to the PSAP.

Since the E9-1-1SSP also has responsibility for the LSRG, it will have visibility into whether a location dereference request initiated by an egress LSRG toward an originating network (i.e., via Demarc Point 20) or toward an LNG (i.e., via Demarc Point 19) resulted in the successful return of location information to the LSRG. The E9-1-1SSP will also be able to determine whether location information was successfully delivered to the legacy PSAP via the ALI system.

10.4.2.3 Callback Information Delivery Failures

10.4.2.3.1 Failures Detected by Originating Network Providers

IP-based originating network providers will have the ability to determine whether outgoing signaling delivered to an NG Emergency Services Network (via Demarc Point 3) includes callback information, but they will not be able to detect whether the callback information was successfully delivered to an egress LSRG or PSAP.

The ability for a legacy originating network to detect failures in the delivery of callback information in an architecture where emergency calls are delivered to legacy PSAPs by SRs that are connected to NG Emergency Services Networks via egress LSRGs will be the same as described in *Section* 10.2.3.1, with the following clarification. Legacy wireline originating

network providers and legacy wireless originating network providers that use the NCAS method will be able to determine whether outgoing MF or SS7 signaling delivered to an LNG (i.e., via Demarc 1) includes an MF ANI or SS7 Calling Party Number, but they will not be able to detect whether the callback information was successfully delivered to an egress LSRG or PSAP. If the legacy originating network provider also operates the LNG, it will be able to determine whether the SIP signaling delivered to the NG Emergency Services Network (via Demarc Point 3) includes callback information, but they will not be able to detect whether the callback information was successfully delivered to an egress LSRG or PSAP.

10.4.2.3.2 Failures Detected by NG9-1-1 System Service Providers

NG9-1-1SSPs will be able to determine whether callback information was received in incoming signaling from an IP originating network or LNG, and will also be able detect whether callback information was successfully delivered to an egress LSRG (i.e., via Demarc Point 18), but they will not be able to detect whether callback information was successfully delivered to the PSAP.

10.4.2.3.3 Failures Detected by E9-1-1 System Service Providers

Since the E9-1-1SSP is assumed to also be responsible for operating the egress LSRG, the E9-1-1SSP will have the ability to determine whether or not callback information was included in the incoming SIP signaling received by the egress LSRG from an NG Emergency Services Network (i.e., via Demarc Point 18). The E9-1-1SSP will also be able to determine whether an SS7 Calling Party Number parameter populated with callback information was delivered to the SR by the egress LSRG, as well as whether the SR was able to successfully deliver that callback information to the target PSAP with the call. If the SR fails to receive an SS7 Calling Party Number containing callback information in incoming signaling from the LSRG, and the PSAP expects to receive callback information via the MF interface from the SR, the SR will include a substitute ANI string (e.g., 0-9-1-1-0000 or 000-9-1-1-0000) in the signaling to the PSAP. The E9-1-1SSP will be able to detect whether an ANI failure condition is encountered by an SR.

If the E9-1-1SSP is also the ALI provider, it will be able to detect whether callback information is included in responses to ALI queries steered by the ALI system to the egress LSRG. An E9-1-1SSP that is also an ALI provider will also be able detect whether that callback information was successfully returned by the ALI system to the PSAP.

11 Analysis of Best Practices

The Best Practices review process consisted of a thorough evaluation of the over 1000 existing CSRIC Best Practices by suggesting Best Practices that could be extended to apply to NG9-1-1, identifying potential gaps for which additional Best Practices could be developed, and proposing Best Practices to fill those gaps.

As noted on the FCC Best Practices website [12], traditional framework of CSRIC Best Practices establishes Network types as:

- Cable
- Internet/Data
- Satellite

- Wireless
- Wireline

Industry roles are also described within the CSRIC framework as:

- Service Provider
- Network Operator
- Equipment Supplier
- Government
- Public Safety
- Property Manager

The Working Group focused on identifying gaps in existing CSRIC Best Practices, and recommendations for new Best Practices which could assist in minimizing outages as the legacy 9-1-1 systems are migrated to NG9-1-1. Existing CSRIC Best Practices were evaluated for applicability to NG9-1-1, and gaps were observed. Appendix B provides modified Best Practices and Appendix C provides new Best Practices that relate to the gaps identified with existing Best Practices. Specifically, the Best Practices provided in Appendixes B and C focus on areas that represent the scope and capabilities within the transition from legacy 9-1-1 to advanced Next Generation 9-1-1 IP infrastructures, and the interconnection to NG9-1-1.

Note that the Best Practices identified in Appendix B –Recommended Changes to Existing 9-1-1 Related Best Practices, and in Appendix C –Recommended NEW 9-1-1 Related Best Practices. are representative of (200+) modified and (40) proposed new Best Practices that apply to NG9-1-1.

The Working Group recognized the importance of cyber security for 9-1-1 networks. There have been extensive efforts related to this category in prior FCC initiatives as they apply 9-1-1 and the Working Group yields to the recommendations developed by NIST [10], TFOPA [4], CSRIC III, IV and V (https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council) for these critical reports and applicable Best Practices.

12 Analysis of Network Monitoring/Reporting Tool Research

In June of 2017 the FCC tasked Working Group 1, Task Group 1 with responsibility to make recommendations on improving reliability of both legacy 9-1-1 and NG9-1-1 systems, including the transition to NG9-1-1. For the purpose of this discussion, “systems” refer to the call origination networks, the legacy 9-1-1 systems and the NG9-1-1 systems in terms of stakeholder roles to one or more or the above.

While the charter included many deliverables related to mitigating risks against the threat of outages to both legacy 9-1-1 and NG9-1-1, the FCC sought recommended action to encourage the private sector to detect or deter threats to 9-1-1 before they reach the ESInet perimeter. In line with the FCC charter the focus of this section is to disclose the finding of the Working Group research and identify tools that are already available, or not overly burdensome to implement for carriers and 9-1-1 System Service Providers.

Unfortunately, the term "burdensome" is subject to differing interpretations based on the user circumstances. For this Report the Working Group considered the following to represent examples of burdensome circumstances:

- The recommended / required change will result in significant [9] negative impact to the current year and following 3 years operations and capital budget.
- The recommended / required change will result in a significant negative impact to the operations staff due to the new skill sets and certifications required to operate the new equipment / systems.
- The recommended / required change may result in a significant negative impact to service uptime due to the lack of adequate system redundancy. The change is designed such that it cannot be implemented during the normal contracted maintenance window thus requiring extended system unavailability.

In an effort to identify network tools currently used by the private sector to detect and deter outages, the Working Group conducted research with the private sector industry representatives serving on the Working Group. The goal of the research was to assist with making recommendations regarding "system tools" private sector companies could consider using within their network operations to minimize outages during the transition from Legacy 9-1-1 to NG9-1-1. The research consisted of a series of open-ended questions designed to collect data on existing commercial, or customized, network tools. The research questions are described below:

- What tools do you use to detect, deter and report transport related issues? Are the tools commercially available, or developed internally for your organization?
- What tools do you use to detect and report any routing related issues (E9-1-1 and NG9-1-1 environments)? Are the tools commercially available, or developed internally for your company?
- What tools do you use to detect and report any proxy or other NG9-1-1 related issues? This would apply if you are running any of your own NG9-1-1 functional elements such as a Location Information Server (LIS), Legacy Network Gateway (LNG) or Legacy Selective Router Gateway (LSRG). Are the tools commercially available, or developed internally for your company?
- What tools do you use to detect and report any cyber or information security threat related issues? Are the tools commercially available, or developed internally for the company?
- Which information security management framework(s) (if any) do is applied to NG9-1-1 products and services?
- What other recommendations, tools, key performance indicators or capabilities do you have that will assist in ensuring network reliability and help increase the situational awareness capabilities of the NG9-1-1 Service Providers, 9-1-1 Administrators, and/or PSAPs?

[9] Significant is used herein consistent with previous FCC use of the term "commercially reasonable".

13 Recommendations

The CSRIC VI Working Group 1, Task Group 1 was directed to recommend measures to improve both legacy 9-1-1 and NG9-1-1, 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, maintenance, and to mitigate the threat of outages in both legacy 9-1-1 and NG9-1-1 systems. The FCC also charged the Work Group with recommending 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 Task Group 1 Report contains a thorough discussion and overview of transitional and end-state NG9-1-1 architectures which will aid Service Providers in understanding the complexities of NG9-1-1, and identifying potential points of failure with respect to emergency call delivery, location delivery and callback information delivery to PSAPs. The following recommendations should be considered by Service Providers in order to aid in a smooth transition to NG9-1-1.

13.1 Understanding NG9-1-1 Architectures

There is a need for Service Providers across all industry segments (cable, wireline, wireless, Interconnected VoIP) to be able to identify within their networks service-impacting events that impair or cause a total loss of service. Network events/ anomalies potentially impact 9-1-1 call delivery throughout the country and the Working Group recommends that Service Providers ensure Product Management and Network Operations personnel have a thorough understanding of the functional elements that support the transitional and end-state NG9-1-1 architectures described in this Report in the following sections:

- *Section* 4 describes various entities that have responsibility for managing risks and reporting outages in terms of stakeholder roles that are associated with different components of transitional and end-state NG9-1-1 architectures. These descriptions provide a basis for identifying the types of failures that may be visible to entities operating different components of the NG9-1-1 service architecture.
- *Sections* 5 *through* 9 describe the various components of transitional and end-state NG9-1-1 architectures and define points of demarcation that denote the logical boundaries of responsibility between the stakeholders responsible for providing those components.

These sections provide detailed overviews of the various transitional and end-state NG9-1-1 architectures to establish a framework for the analysis of potential failure points that follows.

13.2 Identifying Risks with The Transition to NG9-1-1

The Working Group studied specific types of failures that originating Service Providers, 9-1-1 System Service Providers and other entities in the 9-1-1 call chain can detect, with the objective of deterring outages before they impact 9-1-1 call and data delivery to PSAPs.

Section 10, Architectural Analysis analyzes the transitional and end-state NG9-1-1 architectures, by demarcation pint and stakeholder role, to identify potential points of failure from the perspective of:

- Call delivery failures,

- Location delivery failures, and
- Callback information delivery failures.

Potential failures in the delivery of other critical information to key architecture elements and PSAPs are also identified through the definition of the demarcation points and the high-level descriptions that comprise the architectural analysis.

This section emphasizes how transitional and end-state NG9-1-1 architectures, by their very nature, limit any given stakeholder's monitoring and reporting capabilities to those aspects of the architecture to which they have visibility.

It is recommended that Service Providers should ensure their Product Management and Network Operations personnel have a thorough understanding of the Architectural Analysis as described in this Report and have a working knowledge of where potential network failures can be experienced.

13.3 Recommended Actions to Detect and Deter Threats To 9-1-1.

In a recent FCC publication, Summary of 9-1-1 Certification Data for 2017, the Public Safety and Homeland Security Bureau reported on 188 covered entities filing certifications consistent with the FCC 9-1-1 certification rules. Service Providers are encouraged to review the findings of the Report which contains aggregate network data from communications Service Providers that offer 9-1-1, E9-1-1 or NG9-1-1 capabilities. The Report also provides insight into measures that are being taken by the industry to enhance the reliability of 9-1-1 networks and those recommendations are incorporated into this document. Additionally, the FCC can assist in the smooth transition from Legacy 9-1-1 to NG9-1-1 by encouraging Service Providers to review in detail the findings in the Summary of 9-1-1 Certification Data for 2017 as well as this CSRIC VI Report. Specific attention should be paid to the network risk findings in *Section* 10, Architectural Analysis.

For Service Providers and other 9-1-1 stakeholders who do not have robust network monitoring systems, the Working Group also recommends reviewing *Section* 12, Analysis of Network Monitoring/Report Tools. Based on research conducted by the Working Group, this section of the Report provides 9-1-1 stakeholders with a better understanding of the various network elements that require monitoring and commercially available tools that can be obtained to manage the various and complex elements of communications networks. The FCC clarified in its directive to determine if tools were commercially available and not burdensome to implement. The Working Group refrained from determining if the implementation of commercially available tools could be burdensome on a Service Provider. However, the Working Group strongly recommends that Service Providers consider incorporating network detection tools, as appropriate, to assist network operations in detecting or deterring threats to 9-1-1 before they reach the ESInet perimeter. The Working Group also recommends that Service Providers and other stakeholders work together to ensure that the system monitoring information that is needed to mitigate risks, monitor elements of the NG9-1-1 infrastructure and identify 9-1-1 outages is shared between providers and that the information is available to stakeholders when needed.

13.4 Best Practices

Working Group 1, Task Group 1 was asked to review existing Best Practices and develop additional guidance regarding overall monitoring, reliability, notifications, and accountability in preventing 9-1-1 outages in transitional NG9-1-1 environments. Existing CSRIC Best Practices were evaluated for applicability to NG9-1-1, gaps were observed, and additional Best Practices were proposed. Specifically, the Working Group performed the following tasks:

- Reviewed existing CSRIC Best Practices regarding overall monitoring, reliability, notifications, and accountability in preventing 9-1-1 outages in transitional NG9-1-1 environments.
- Identified gaps in existing CSRIC Best Practices that should be filled to facilitate the transition to NG9-1-1.
- Developed additional guidance regarding overall monitoring, reliability, notifications, and accountability in preventing 9-1-1 outages in transitional NG9-1-1 environments.
- Made recommendations to protect the NG9-1-1 network, including recommendations for Best Practices and standards development.

13.5 Cybersecurity Considerations

While cybersecurity considerations are an important part of the transition to NG9-1-1, this Report does not focus on cybersecurity. The Working Group recommends that stakeholders take deliberate steps to consider the cybersecurity implications introduced by the transition to NG9-1-1. The Working Group also recommends that a future CSRIC focus on NG9-1-1 related cybersecurity challenges and develop Best Practices as appropriate.

The public safety community must continually identify risks and address evolving physical and cyber security requirements. The rapid rate of technology advancement continues to outpace the public safety community's ability stay ahead of the threats.

The SAFECOM Nationwide Survey (SNS), a public safety data collection effort conducted from January through March 2018, included input from federal, state, local, tribal, territorial, urban and rural communities, as well as across the span of public safety disciplines. Over a third (37 percent) of SNS respondents indicated that cybersecurity incidents had an impact on the ability of their emergency response providers and government officials' ability to communicate over the past five years. Yet, almost half (46 percent) of the organizations had not instituted cybersecurity best practices, such as risk assessment, continuous monitoring, and identity management. In fact, only one in five (20 percent) of the organizations indicated having cybersecurity incident response plans, policies, and capabilities.

Like other aspects of communications, cybersecurity is a shared responsibility. All levels of government, private and nonprofit sectors, and individual citizens must work together to protect voice and data communications. Ideally, each organization would employ an enterprise-wide, risk-informed cybersecurity management program with continuous improvement and coordination with all interconnected systems and the broader community.

The *National Institute of Standards and Technology's (NIST) Cybersecurity Framework* [10] is a flexible, risk-based approach to improving the security of critical infrastructure.

Collaboratively developed between government and the private sector, the Framework is designed to complement an existing risk management process or to develop a credible program if one does not exist. Governance is explicitly addressed within the Framework, and resources are provided to establish and communicate the necessary governance structures (e.g., risk councils) and organizational cybersecurity policy for risk management.

Appendix-B Table B-3 of the SAFECOM document titled "FY 2019 SAFECOM Guidance on Emergency Communications Grants", provides a list of Cybersecurity Resources. The document was created by the SAFECOM Funding and Sustainment Committee. The committee is made up of members of the Emergency Response Community supported by Federal Office of Emergency Communications Staff. That table is included here for convenience.

Table B-3. Cybersecurity Resources

Organizations	Resources
Committee on National Security Systems (CNSS)	• CNSS Policies
Department of Homeland Security	• C^3 Voluntary Program Cyber Resilience Review • Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan • Continuous Diagnostics and Mitigation (CDM) • Cybersecurity Evaluation Tool (CSET) • Emergency Services Sector (ESS) Cyber Risk Assessment – 2012 • ESS Roadmap to Secure Voice and Data Systems – 2014 • ESS Cybersecurity Framework Implementation Guidance – 2015 • Emergency Services Sector-Specific Tabletop Exercise Program (ES SSTEP) • Homeland Security Grant Program Supplemental Resource: Cyber Security Guidance • Intrusion Detection (IDS) and Intrusion Prevention (IPS) • Information Sharing Environment (ISE) Guides and Best Practices • National Cyber Incident Response Plan • National Cybersecurity and Communications Integration Center (NCCIC) and U.S. Computer Emergency Readiness Team (US-CERT) • National Infrastructure Coordinating Center (NICC) • National Infrastructure Protection Plan • Network Flow Collection • Safeguarding and Securing Cyberspace • Supplement Tool: Executing a Critical Infrastructure Risk Management Approach • Supplement Tool: National Protection and Programs Directorate Resources to Support Vulnerability Assessments • Trusted Internet Connections • Guidelines for Encryption in Land Mobile Radio Systems • Best Practices for Encryption in Project 25 Public Safety Land Mobile Radio Systems
Department of Energy	• Energy Sector Cybersecurity Capability Maturity Model (C2M2) Program

Organizations	Resources
Executive Orders (EO) and President Directives	• EO 13636: Improving Critical Infrastructure Cybersecurity • EO 13231: Critical Infrastructure Protection in the Information Age and EO 13286 • EO 13618: Assignment of national Security and Emergency Preparedness Communications Functions • Executive Office of the President, Presidential Policy Directive 21 (PPD – 21) • EO 13407: Public Alert and Warning System
Federal Bureau of Investigation	• Internet Crime Complaint Center
Federal Communications Commission	• Communications Security, Reliability and Interoperability Council (CSRIC) • Task Force on Optimal PSAP Architecture (TFOPA) • Cyber Security Planning Guide
Federal Emergency Management Agency	• Emergency Management and Response-Information Sharing and Analysis Center (EMR-ISAC)
Government Accountability Office	• U.S. Government Accountability Office, Cybersecurity
National Institute of Standards and Technology	• Framework for Improving Critical Infrastructure Cybersecurity • Internal/Interagency Reports (NISTIRs) • National Initiative for Cybersecurity Education (NICE) • NICE Cybersecurity Workforce Framework
Various Industry and Associations	• ATIS Industry Best Practices • Association of Public-Safety Officials, International (APCO), specifically SPCO Cybersecurity Guide for Public Safety Community Professionals and APCO Introductory Guide to Cybersecurity for PSAPs ISACA COBIT 5 Framework • ITU Security Standards Roadmap • SANS Institute 20 Critical Security Controls • National Association of State Chief Information Officers (NASCIO) Cybersecurity Awareness, including NASCIO Cyber Disruption Planning Guide for States • National Conference of State Legislation Cybersecurity Training for State Employees • Open Web Application Security Project (OWASP) Top Ten Project • OWASP Internet of Things Project

Other Cybersecurity resources are listed in the References section. Those include:

- DHS - Cyber Risks to Next Generation 911 [16]
- FTC – Cybersecurity for Small Business [17]

13.6 Research Findings

The scope of the research was a small sampling of Working Group 1, Task Group 1 Private Sector Industry stakeholders. The information received was determined to be relevant in answering the FCC's question, "Are there tools commercially available that can detect or deter to mitigate an outage?".

The matrix in Appendix A – Aggregated Research Inquiry Results summarizes the response to the research and provides information on tools used to detect, deter and mitigate network anomalies within the 9-1-1 networks infrastructure. There are commercially available tools the private sector can deploy to assist in detecting, deterring or mitigating outages within the 9-1-1 systems. Recognizing companies need to have tools in place to manage their networks, the tools companies elect to have in place to assist in managing the networks are company specific and depend on budgetary parameters, as well as available resources.

In a recent publication, Summary of 9-1-1 Certification Data for 2017, the Public Safety and Homeland Security Bureau reported on 188 covered entities filing certifications consistent with the 9-1-1 certification rules. The Report contains aggregate network data from communications Service Providers that offer 9-1-1, E9-1-1 or NG9-1-1 capabilities such as call routing, automatic location information, and automatic number identifies directly to a public safety answering point. The following are the highlights of the FCC findings, and the Working Group encourages companies to review the Report in its entirety [13]:

- *"Of the 188 covered entities that filed certifications, 48 certified that they have diverse 9-1-1 circuits to all PSAPs to which they provide 9-1-1 circuits. Twenty covered entities certified that they have implemented alternative measures in lieu of circuit diversity for all of the PSAPs that they serve. Fifteen covered entities certified that they provide diverse 9-1-1 circuits to some PSAPs and that they have implemented alternative measures to other PSAPs to which they provide 9-1-1 circuits.*
- *"There were 6,769 unique PSAPs listed in the certifications for 9-1-1 circuit diversity. The certifications showed that of these 6,769 PSAPs, 3,855 PSAPs had diverse circuits and 2,914 had implemented alternative measures.*
- *"Of the 188 covered entities that filed certifications, 165 indicated that they have certified backup power in all central offices that serve PSAPs. Nine certified that they have alternative measures for backup power in all such central offices, and four covered entities certified that they have back-up power in some central offices and have implemented alternative measures in all other central offices.*
- *"Of 188 covered entities that filed certifications, 51 stated that they have diverse monitoring in all of their 9-1-1 service areas, and ten stated that they have certified alternative measures in all 9-1-1 service areas. Seven covered entities certified that they provide diverse monitoring in some of their 9-1-1 service areas and have implemented alternative measures in all other 9-1-1 service areas."*

As the United States migrates to a nationwide Next Generation 9-1-1 infrastructure, private sector companies operating within the 9-1-1 ecosystem should have a thorough understanding of Commission rules, recommended Best Practices and industry network tools that are designed to ensure the reliability of the 9-1-1 infrastructure, and mitigate risks.

14 Conclusions

CSRIC VI, Working Group 1, Task Group 1 is pleased to submit this Report which meets the Objectives set forth by the FCC as follows:

- Reviewed existing Best Practices regarding overall monitoring, reliability, notifications, and accountability in preventing 9-1-1 outages in transitional NG9-1-1 environments.
- Developed and recommended the modification and addition of Best Practices regarding overall monitoring, reliability, notifications, and accountability in preventing 9-1-1 outages in transitional NG9-1-1 environments.
- Identified risks associated with transitional 9-1-1 systems that could result in disruptions to 9-1-1 service.
- Studied specific actions that originating Service Providers, 9-1-1 System Service Providers and other entities in the 9-1-1 call chain should take to detect and deter outage precursors before 9-1-1 calls are delivered to the ESInet gateway.
- Recommended actions the FCC could take to encourage the private sector stakeholders to detect or deter threats to 9-1-1 with a focus on identifying tools that are available for the various network components, and that may be commercially available.

The Working Group is comprised of some of this country's foremost 9-1-1 industry Subject Matter Experts. Through the dedication of this team the Report provides extensive educational insight into the various elements of transitional and end-state Next Generation 9-1-1 architectures, with attention to details on potential outage risks. As our Nation transitions from a legacy 9-1-1 circuit-switched service architecture to an NG9-1-1 IP-based service architecture, this Report will aid all 9-1-1 stakeholders in understanding the core elements of the transition. It is recommended that Service Providers ensure their Network Operations and Product Management personnel are aware of the complexities associated with transitioning to NG9-1-1. It is important to understand the importance of the collaboration needed between all stakeholders in order to help facilitate a smooth transition to NG9-1-1. Stakeholders should also consider this Report as an opportunity to assess their own networks, and review all the functional elements involved in the transition and ensure the reliability and resiliency of those networks.

15 Appendix A – Aggregated Research Inquiry Results

The Working Group queried Private Sector Industry stakeholders regarding the use of tools for Network Monitoring/Reporting. The information received was determined to be relevant in answering the FCC's question, "Are there tools commercially available that can detect or deter to mitigate an outage?". The matrix in this Appendix summarizes the response to the research and provides information on tools used to detect, deter and mitigate network anomalies within the 9-1-1 networks infrastructure.

Research Inquiry #1:

What tools do you use to detect, deter and report transport related issues? Are those tools commercially available, or developed internally for your organization?

Tool Description	Summary Description	Commercially Available (Y/N)
Fault Management System	Fault management systems can be considered off the shelf software. Depending on the size of the organization there is a substantial investment required from a licensing and support perspective.	Yes
Network Traffic Management/Monitoring	Real-time network transaction monitoring tools are commercially available and includes auto discovery, service mapping, dashboards alerts and archived data retrieval.	Yes
Remote Terminal Units	Central Office/Data Centers are monitored by remote terminal units (RTU's) that collect informational, observational, major, critical personnel, access/occupancy, generator, environmental and power status conditions in real time.	Yes
Network / Transport Monitoring	Commercially available tools and protocols used to administer, operate, and monitor transport elements include the native NMS and provisioning systems of the vendor platform itself.	Yes
Network Management Protocol	Transaction Language 1 (TL1) is a widely used management protocol in telecommunications which allows a human or OSS (Operations Support System) to manage a network element and its resources. Simple Network Management Protocol - SNMP is based on industry standards for collecting and organizing information about managed devices on IP network.	Yes
Network Visibility, Traffic Analysis	Commercially available solutions provide network visibility, traffic analysis, and can be leveraged for application and network performance management.	Yes
Softswitch Software	SIP Session Border Controller (SBC) performance and alarms measured from softswitch software vendor.	Yes
Metrics & Ticketing Systems	Reporting system can be deployed for additional metrics if needed. Ticketing systems are available with off the shelf software, that requires internal customization to enable automation of work flow processes. Research also revealed companies use customized tools.	Yes/Customized

2420
2421

Research Inquiry #2:

What tools do you use to detect and report routing related issues? (E9-1-1 and NG9-1-1 Environments)? Are those tools commercially available, or developed internally?

Tool Description	Summary Description	Commercially Available (Y/N)
Fault Management System	Fault management systems can be considered off the shelf software. Depending on the size of the organization there is a substantial investment required from a licensing and support perspective.	Yes
Network Traffic Management/Monitoring	Real-time network transaction monitoring tools are commercially available and includes auto discovery, service mapping, dashboards alerts and archived data retrieval.	Yes
Softswitch Monitoring	Commercially available solution that provides monitoring of the softswitch.	Yes
Network Visibility, Traffic Analysis	Commercially available solution that provides network visibility, traffic analysis, and can be leveraged for application and network performance management.	Yes
Voice Network End to End Visibility	Commercially available tool that provides end to end visibility within the Voice Network	Yes
Network Routing	Standard IP Network Routing alarming and reporting methods would be used.	Yes
Call Routing/Softswitch	Call routing reporting provided by softswitch vendor.	Yes /With Customization
Signaling Packet Analysis	Commercially available tools for voice networks which collect signaling, rules applied, and routing decision made by individual network functions and stores them for proactive analysis and deep packet protocol decoding.	Yes
Application Performance/Configuration Management	Commercially Available tool. Application performance monitoring and configuration management tool	Yes
IP/Ethernet Data	Standard IP/Ethernet SNMP and NMS statistical data	Yes
Ticketing Systems	Off the shelf software, that requires internal customization to enable automation of work flow processes. Research also revealed companies use customized tools.	Yes /With Customization

Research Inquiry #2:

What tools do you use to detect and report routing related issues? (E9-1-1 and NG9-1-1 Environments)? Are those tools commercially available, or developed internally?

Tool Description	Summary Description	Commercially Available (Y/N)
Data Analytics	Off the shelf data analytics tool. There is a considerable amount of data mining and customization required for any organization. While there can a heavy cost to the use of this analytics engine the output is proving to be critical in gaining that timely identification of real impacts.	Yes
PSAP Impact Tool	Customized application that uses data analytics engine to identify PSAPs and calls impacted during an outage situation.	No, but works with Commercial Tool

2422
2423

Research Inquiry #3:

What tools do you use to detect and report any proxy or other NG9-1-1 related issues? (This would apply if you are running any of your own NG9-1-1 functional elements such as a Location Information Server (LIS), Legacy Network Gateway (LNG) or Legacy Selective Router Gateway (LSRG).) Are these tools commercially available, or developed internally?

Tool Description	Summary Description	Commercially Available (Y/N)
Fault Management System	Fault management systems can be considered off the shelf software. Depending on the size of the organization there is a substantial investment required from a licensing and support perspective.	Yes
Application Performance/Configuration	Commercially available. Application performance monitoring and configuration management tool.	Yes
Network Visibility, Traffic Analysis	Commercially available solution that provides network visibility, traffic analysis, and can be leveraged for application and network performance management.	Yes
Voice Network End to End Visibility	Commercially available tool that provides end to end visibility within the voice network.	Yes
Softswitch vendor software.	Commercially available tool that provides end to end visibility within the voice network.	Yes
SNMP and alarm collection system.	Devices and software which provide network data collection, network health management, and remediation.	Yes
Ticketing Systems	Off the shelf software, that requires internal customization to enable automation of work flow processes.	Yes, With Customization

Research Inquiry #3:

What tools do you use to detect and report any proxy or other NG9-1-1 related issues? (This would apply if you are running any of your own NG9-1-1 functional elements such as a Location Information Server (LIS), Legacy Network Gateway (LNG) or Legacy Selective Router Gateway (LSRG).) Are these tools commercially available, or developed internally?

Tool Description	Summary Description	Commercially Available (Y/N)
Data Analytics	Off the shelf data analytics tool. There is a considerable amount of data mining and customization required for any organization. While there is a heavy cost to the use of this analytics engine the output is proving to be critical in gaining that timely identification of real impacts.	Yes
PSAP Impact Tool	Customized application that uses the data analytics engine to identify PSAPs and calls impacted during an outage situation.	No, but works with Commercial Tool
PSAP Data, Route, Operational Tool	MP – Internally developed Management Portal. • Provision PSAP contact information and feature subscription information • Provision PSAP route and abandonment list • PSAP operational state • Abandonment route list • Fixed transfer and bridge list • ESN selective bridge list • Statewide PSAP directory • CDRs	No
	ESInet Packet Capture Tool - internally developed and used to capture packets for analysis on NG9-1-1 networks.	No
Research Inquiry #3 continued below		
Carrier Management Portal for PSAP Data, Network route, and operational data	Customized Carrier Management Portal is a web-based application that allows authorized personnel from carriers, regional agencies, or PSAPs to view, through a single sign-on, the following information for one or more PSAP-level accounts deployed on the company ESInet: • Provisioned PSAP contact information and feature subscription information • PSAP operational state • Abandonment route list • Fixed transfer and bridge list • ESN selective bridge list • Statewide PSAP directory • CDRs	No

Research Inquiry #3:

What tools do you use to detect and report any proxy or other NG9-1-1 related issues? (This would apply if you are running any of your own NG9-1-1 functional elements such as a Location Information Server (LIS), Legacy Network Gateway (LNG) or Legacy Selective Router Gateway (LSRG).) Are these tools commercially available, or developed internally?

Tool Description	Summary Description	Commercially Available (Y/N)

2424

Research Inquiry #4:

What tools do you use to detect and report any cyber or information security threat related issues? Are these tools commercially available, or developed internally?

Tool Description	Summary Description	Commercially Available (Y/N)
Firewall Alarming	SIP based firewall alarming session border controller and data firewall alarming.	Yes
Traffic Alarming	SIP Traffic and session volume threshold and anomaly alarming	Yes
Network Elements	Authentication Network Element Tools	Yes
DOS Detection Tools	Traffic analyzer tools which assist with DoS detection and reporting	Yes
Anti-Virus/Malware Tools	Tools which detect and prevent malicious software from being installed on servers and workstations.	Yes

2425

2426

Research Inquiry #5:

Which information security management framework(s) (if any) do you apply to your NG9-1-1 products and services?

Tool Description	Summary Description	Commercially Available (Y/N)
Information Security Management Framework	NIST Framework	n/a
Security Frameworks	Security and Policy Requirements	n/a

2427
2428

Research Inquiry #6:

What other recommendations, tools, key performance indicators or capabilities do you have that will assist in ensuring network reliability and help increase the situational awareness capabilities of the NG9-1-1 Service Providers, 9-1-1 Administrators, and/or PSAPs?

Tool Description	Summary Description	Commercially Available (Y/N)
PSAP, 9-1-1 Authority Database	Internally developed tool that provides PSAP contact information, location, SR, and PSAP authority contact information.	No
9-1-1 Network Data	Tools that identify all characteristics associated with 9-1-1 call and outage impacts.	No
	Recommend utilizing next generation network monitoring tools and network probes for NG9-1-1 networks.	Yes
	Recommend PSAPs establish standard configurations with requirements for hardware and naming. This will enable correlation and automation to expedite detection of events and ensure that there is redundancy to enable failover.	n/a
Automated PSAP Notification	Commercially available tool that provides the ability to automate PSAP and employee notifications.	Yes
Information Sharing	A Portal supporting a common collaboration and information exchange.	Unknown

2429
2430

16 Appendix B –Recommended Changes to Existing 9-1-1 Related Best Practices

The Best Practices in this Appendix are existing Best Practices that were modified based upon the analysis of the Working Group. The *final* recommended text is shown in this Appendix.

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-10-1068	Network Operators, Service Providers, Property Managers and Public Safety should utilize Transfer Switch Equipment that conforms to industry standards.	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-1069	Network Operators, Equipment Suppliers, Property Managers and Public Safety should consider marking or modifying copper bars and cable to deter theft, to make them easier to identify at scrap yards, and/or to reduce their value.	TRUE	TRUE	FALSE	TRUE	FALSE	TRUE
11-10-5029	Network Operators, Service Providers, Equipment Suppliers, Property Managers and Public Safety should facilitate the availability of security related hardware and media (e.g., spare hardware) and/or a contingency plan for its availability in the event of a disaster.	TRUE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5040	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should install environmental emergency response equipment (e.g., fire extinguishers, high rate automatically activated pumps) where appropriate, and periodically inspect the equipment in accordance with local codes.	TRUE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-10-5048	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should implement a policy that requires approval by senior member(s) of the organization for security related goods and services contracts.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5052	Network Operators, Service Providers, Equipment Suppliers, Property Managers and Public Safety using guard services should ensure that each post has written detailed post orders including site specific instructions, up-to-date emergency contact information and ensure that on the job training occurs.	TRUE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8691	Cybersecurity Awareness: Network Operators, Service Providers, Public Safety and Equipment Suppliers should develop or adopt employee education programs that emphasize the need to comply with security policies.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-0805	Service Providers, Network Operators, Public Safety and Equipment Suppliers should work to establish operational standards and practices that support broadband capabilities and interoperability (e.g., video, voice, data, wireless).	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-9-0900	Network Operators and Service Providers operating a VoIP Positioning Center (VPC), Mobile Positioning Center (MPC), or Gateway Mobile Location Center (GMLC) should strive to reduce missing or malformed shell record data routing errors for 9-1-1 pseudo Automatic Number Identification (pANI) due to incorrect Master Street Address Guide (MSAG) to Emergency Service Number (ESN) to Public Safety Answering Point (PSAP) relationship (MSAG-ESN-PSAP) by following National Emergency Number Association (NENA) 56-504 "NENA VoIP 9-1-1 Deployment and Operational Guidelines" to fully test routing for every pANI placed in service.	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE
11-11-0901	Network Operators, Service Providers and Public Safety should conduct extensive 9-1-1 call-through testing for environments that have a high user capacity (e.g., university campuses, large commercial enterprise campuses, and densely populated multi-tenant buildings/complexes) to immediately reduce the risk of misrouting a block of callers at a particular facility.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-11-0902	Originating Network Operators and Service Providers should assess the impact on the routing of 9-1-1 calls when reconfiguring their networks. Such reconfiguration may include: making changes to VoIP Positioning Centers (VPCs), Mobile Position Centers (MPCs), Gateway Mobile Location Centers (GMLCs), and Emergency Services Gateways (ESGWs); rehoming trunking to Legacy Network Gateway(s) (LNGs); and/or establishing IP connections to Border Control Functions (BCFs).	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0764	Network Operators, Service Providers and Public Safety should implement congestion control mechanisms.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-6-3203	Network Operators, Service Providers and Public Safety should consider developing options that allow for call delivery from Emergency Notification Services to subscribers with call blocking/screening services in order to assist in the effectiveness of Emergency Notification Systems (Public Safety Mass Calling) and return calls from PSAPs.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-5049	Network Operators, Service Providers, Equipment Suppliers, Property Managers and Public Safety should consider a strategy of using technology (e.g., access control, CCTV, sensor technology, person traps, turnstiles) to supplement the guard services.	TRUE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5050	Network Operators, Service Providers, Equipment Suppliers, Public Safety and Property Managers utilizing guard services should have a supervision plan that requires supervisory checks for all posts.	TRUE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5051	Network Operators, Service Providers, Public Safety and Equipment Suppliers utilizing guard services should consider establishing incentives and recognition programs to increase morale and reduce turnover.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5054	Network Operators, Service Providers, Equipment Suppliers, Public Safety and Property Managers utilizing guard services should develop a process to quickly disseminate information to all guard posts. This process should be documented and should clearly establish specific roles and responsibilities.	TRUE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-10-5055	Network Operators, Service Providers, Public Safety and Equipment Suppliers should establish and maintain (or contract for) a 24/7 emergency call center for internal communications. Ensure staff at this center has access to all documentation pertinent to emergency response and up to date call lists to notify appropriate personnel. The number to this call center should be appropriately published so personnel know where to report information.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5097	Network Operators, Service Providers, Public Safety and Equipment Suppliers should establish and implement standards for physical and system security requirements in consideration of the Best Practices of the communications industry.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5098	Network Operators, Service Providers, Public Safety and Equipment Suppliers should ensure that all network infrastructure equipment meets the minimum industry standards for fire resistance.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5168	Network Operators, Service Providers, Public Safety and Equipment Suppliers should review personnel background information prior to assignment to sensitive roles, to ensure there are no security risks, or risk of compromising processes as they evolve.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5172	Network Operators, Service Providers, Public Safety and Equipment Suppliers should not permit unsecured wireless access points for the distribution of data or operating system upgrades during normal operations or system restoration efforts.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5243	Network Operators, Service Providers, Public Safety and Equipment Suppliers should consider restricting, supervising, and/or prohibiting tours of critical network facilities, restoration sites and operations.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5244	Network Operators, Service Providers, Public Safety and Equipment Suppliers should make all employees, contractors, and others with access to critical infrastructure during restoration, aware of changes to security posture resulting from the incident, and the need for increased vigilance.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-10-5249	Network Operators, Public Safety and Service Providers should consider geographic separation of network redundancy during restoration, and address losses of redundancy and geographic separation following restoration.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-6-8102	Regarding the use of Personal Equipment for Corporate Activities, Network Operators, Service Providers, Public Safety and Equipment Suppliers should provide adequate security and control of devices used for telecommuting, virtual office, remote administration, etc.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-7-0491	Network Operators, Service Providers, Public Safety and Equipment Suppliers should, where programs exist, coordinate with local, state and/or federal emergency management and law enforcement agencies for pre-credentialing to help facilitate access by technicians to restricted areas during an event.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-0494	Network Operators and Property Managers should consider including a provision in cell-site contracts for back-up power.	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
11-7-0497	Network Operators, Public Safety and Property Managers should consider connecting the power load to portable generators stored at critical sites, and configuring them for auto-engage in the event of a failover.	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE
11-10-0499	Network Operators and Service Providers should consider ensuring that the back-haul facility equipment located at the cell site is provided with backup power duration equal to that provided for the other equipment at the cell site.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0508	Network Operators, Public Safety and Service Providers should establish company-specific interconnection agreements, and where appropriate, utilize existing interconnection templates and existing data connection trust agreement.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-7-0518	Capacity Monitoring: Network Operators, Public Safety (for NG9-1-1) should design and implement procedures for traffic monitoring, trending and forecasting so that capacity management issues may be understood.	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE
11-7-0521	Industry Standards: Network Operators, Public Safety, Service Providers and Equipment Suppliers should work toward implementing industry standards for interconnection points.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-7-0522	Industry Forum Participation: Network Operators, Service Providers, Public Safety and Equipment Suppliers should participate in standards development organizations and industry forums.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-0543	Network Operators, Public Safety and Service Providers should establish agreements with Property Managers for both regular and emergency power.	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0588	Network Operators, Public Safety and Service Providers and Equipment Suppliers should provide awareness training that stresses the services impact of network failure, the risks of various levels of threatening conditions and the roles components play in the overall architecture.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-0609	Network Operators, Public Safety and Service Providers should provide and maintain the contact information for mutual aid coordination for inclusion in mutual aid processes.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0618	Network Operators, Public Safety and Service Providers should establish mutually agreed upon reliability thresholds with Equipment Suppliers for new hardware (e.g., routers, switches, call servers, signaling servers) brought into service on the network.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-0629	Network Operators, Public Safety, Service Providers and Property Managers should ensure that a training program is implemented for contractors working in critical equipment locations to ensure they understand the need to protect the continuity of service and all fire safety requirements applicable to the facility.	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0692	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider using fail-safe alarm points with backup power for critical alarms.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-7-0744	Network Operators, Public Safety and Equipment Suppliers should periodically review the results of root cause analysis to ensure that the least impacting methods for fault recovery are being used.	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
11-10-0747	Network Operators, Public Safety, Service Providers and Equipment Suppliers should work together to establish reliability and performance objectives.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-0771	Network Operators, Public Safety, Service Providers and Equipment Suppliers should have a procedure for pre-notification of visits to critical facilities.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-0772	Where applicable, collocated Service Providers, Public Safety, Network Operators and Property Managers should coordinate with collocated entities on equipment moves, adds or changes which could impact other occupants.	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0779	Network Operators, Service Providers, Public Safety and Equipment Suppliers should establish a means to allow for coordination between cyber and physical security teams supporting preparedness, response, investigation and analysis.	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE
11-10-0814	Network Operators, Public Safety (for NG9-1-1) and Service Providers should design broadband networks with the ability to take active measures to detect and restrict or inhibit any network activity that adversely impacts performance or security.	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE
11-10-0820	Network Operators, Public Safety (for NG9-1-1) and Service Providers should deploy networks and services in a manner that mitigates the effects of harmful interference from other sources, and mitigates harmful interference into other services.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0821	Network Operators, Public Safety, Service Providers and Property Managers should coordinate to ensure that network deployment and equipment installation, including equipment moves, adds or changes (MACs), do not physically impair the operation of other collocated communications networks/equipment.	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0822	Network operators, Public Safety and service providers should incorporate multilevel security schemes for network data integrity in the network design, as applicable, to prevent user traffic from interfering with network operations, administration, and management.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-10-1008	Network Operators, Service Providers, Public Safety and Equipment Suppliers should use the Incident Command System for incident coordination and control in the emergency operations center and at the incident site.	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE
11-7-1064	Network Operators, Public Safety (for NG9-1-1) Service Providers and Equipment Suppliers should implement minimum network management controls in order to promote reliability of the interconnected network.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-7-3232	Handsets that use a Global Positioning System (GPS) algorithm for-9-1-1: Equipment Suppliers should ensure that the Phase II handsets commence Global Positioning System (GPS) acquisition before the GPS satellite location identification information is received so that GPS acquisition time is minimized and to reduce the number of database query rebids.	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE
11-10-5001	Network Operators, Property Managers, Public Safety, Service Providers and Equipment Suppliers should establish additional access control measures that provide two factor identification (e.g., cameras, PIN, biometrics) in conjunction with basic physical access control procedures at areas of critical infrastructure, as appropriate, to adequately protect the assets.	TRUE	TRUE	FALSE	TRUE	TRUE	TRUE
11-7-5006	Network Operators, Service Providers, Public Safety, Equipment Suppliers and Property Managers should have policies and procedures that address tailgating (i.e. following an authorized user through a doorway or vehicle gateway). At critical sites, consider designing access points to minimize tailgating.	TRUE	TRUE	FALSE	TRUE	TRUE	TRUE
11-7-5015	Network Operators, Service Providers, Public Safety and Equipment Suppliers should establish separation policies and procedures that require the return of all corporate/agency property and invalidate access to all resources (physical and logical) to coincide with the separation of employees, contractors and vendors.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5018	Network Operators, Public Safety, Service Providers and Equipment Suppliers should periodically conduct reviews to ensure that proprietary information is protected in accordance with established policies and procedures.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-10-5053	Network Operators, Public Safety, Service Providers, Equipment Suppliers and Property Managers should periodically audit guard services to ensure satisfactory performance, and compliance with organizational contractual requirements.	TRUE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5068	Network Operators, Service Providers, Public Safety and Property Managers should establish standards, policies and procedures that, where feasible, restrict equipment access to authorized personnel where co-location exists.	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-5071	Network Operators, Service Providers and Property Managers should maintain liaison with Public Safety, local law enforcement, fire department and other security and emergency agencies to exchange critical information related to threats, warnings and mutual concerns.	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-5096	Network Operators, Public Safety, Service Providers and Equipment Suppliers should require compliance with corporate/agency security standards and programs for contractors (and their subcontractors), vendors and others as appropriate.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5100	Network Operators, Public Safety, Service Providers and Equipment Suppliers should interact with federal, state, and local agencies to identify and address potential adverse security and service impacts of new laws and regulations (e.g., exposing vulnerability information, required security measures, fire codes).	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE
11-7-5107	Network Operators, Public Safety (for NG9-1-1), Service Providers and Equipment Suppliers should evaluate and manage risks (e.g., alternate routing, rapid response to emergencies) associated with a concentration of infrastructure components.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5138	Network Operators and Public Safety should plan for the possibility that impacted network nodes cannot be accessed by company personnel for an extended period of time and define the corporate/agency response for restoration of service.	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE
11-10-5151	Network Operators, Public Safety, Service Providers and Property Managers located in the same facility should coordinate security matters and include all tenants in the overall security and safety notification procedures, as appropriate.	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-10-5153	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should ensure that critical information being provided to outside entities as part of bid processes is covered under non-disclosure agreements and limited to a need to know basis.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5158	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider unannounced internal security audits at random intervals to enforce compliance with company/agency security policies.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5164	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should establish and enforce a policy to immediately report stolen or missing company/agency vehicles and trailers to the appropriate authorities.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5226	Network Operators, Service Providers and Property Managers should maintain liaison with Public Safety and local law enforcement, fire department, other utilities and other security and emergency agencies to ensure effective coordination for emergency response and restoration.	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-5269	Network Operators, Service Providers, Equipment Suppliers, Public Safety and Property Managers should incorporate various types of diversionary tactics into exercises to assess the security response.	TRUE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-5282	Network Operators, Public Safety and Service Providers should coordinate with Property Managers to ensure adequate growth space.	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE
11-7-8029	Network Access to Critical Information: Network Operators, Public Safety and Service Providers and Equipment Suppliers should carefully control and monitor the networked availability of sensitive security information for critical infrastructure by: Periodic review public and internal website, file storage sites HTTP and FTP sites contents for strategic network information including but not limited to critical site locations, access codes. Documenting sanitizing processes and procedures required before uploading onto public internet or FTP site. Ensuring that all information pertaining to critical infrastructure is restricted to need-to-know and that all transmission of that information is encrypted. Screening, limiting and tracking remote access to internal information resources about critical infrastructure.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-7-8067	Evidence Collection Guidelines: Network Operators, Service Providers and Public Safety should develop a set of processes detailing evidence collection and preservation guidelines. Procedures should be approved by management/legal counsel. Those responsible for conducting investigations should test the procedures and be trained according to their content. Organizations unable to develop a forensic computing capability should establish a relationship with a trusted third party that possesses a computer forensics capability. Network Administrators and System Administrators should be trained on basic evidence recognition and preservation and should understand the protocol for requesting forensic services.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-7-8084	Create Trusted PKI Infrastructure When Using Generally Available PKI Solutions: When using digital certificates, Network Operators, Service Providers, Equipment Suppliers and Public Safety (for NG9-1-1) should create a valid, trusted PKI infrastructure, using a root certificate from a recognized Certificate Authority or Registration Authority. Assure your devices and applications only accept certificates that were created from a valid PKI infrastructure. Configure your Certificate Authority or Registration Authority to protect it from denial of service attacks.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-7-8089	Conduct Risk Assessments to Determine Appropriate Security Controls: Network Operators, Public Safety, Service Providers and Equipment Suppliers should perform a risk assessment of all systems and classify them by the value they have to the company/agency, and the impact to the company/agency if they are compromised or lost. Based on the risk assessment, develop a security policy which recommends and assigns the appropriate controls to protect the system.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-7-8091	Protect Cached Security Material: Network Operators, Service Providers, Public Safety and Equipment Suppliers should evaluate cache expiration and timeouts of security material (such as cryptographic keys and passwords) to minimize exposure in case of compromise. Cached security material should be immediately deleted from the cache when the cached security material expires.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-7-8110	News Disinformation: Information from news sources may be spoofed, faked, or manipulated by potential attackers. Network Operators, Service Providers, Public Safety and Equipment Suppliers should ensure news sources are authenticated and cross-verified to ensure accuracy of information, especially when not from a trusted source.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-7-8123	Handle Policy Violations Consistently: Network Operators, Service Providers, Public Safety and Equipment Suppliers should handle violations of policy in a manner that is consistent , and, depending on the nature of the violation, sufficient to either deter or prevent a recurrence. There should be mechanisms for ensuring this consistency.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-7-8521	Recover from Misuse of Equipment for Remote Access of Corporate/Agency Resources: In the event of misuse or unauthorized use in a remote access situation contrary to the AUP (Acceptable Use Policy), Network Operators, Public Safety and Service Providers should terminate the VPN (Virtual Private Network) connection and issue a warning in accordance with the employee code of conduct. If repeated, revoke employee VPN remote access privileges.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-7-8567	News Disinformation after Recovery: Network Operators, Public Safety, Service Providers and Equipment Suppliers should ensure that actions taken due to a spoofed, faked or distorted news item should be cross-correlated against other sources. Any actions taken should be 'backed out' and corrective measures taken to restore the previous state. News source authentication methods should be implemented to ensure future accuracy.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-0507	Attack Trace Back: Service Providers, Network Operators, Equipment Suppliers and Public Safety (for NG9-1-1) should have the processes and/or capabilities to analyze and determine the source of malicious traffic, and then to trace-back and drop the packets at, or closer to, the source. The references provide several different possible techniques. (Malicious traffic is that traffic such as Distributed Denial of Service (DDoS) attacks, smurf and fraggle attacks, designed and transmitted for the purpose of consuming resources of a destination of network to block service or consume resources to overflow state that might cause system crashes).	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0551	Network Operators should design their SS7 network components and interfaces consistent with industry base security guidelines to reduce the risk of potentially service affecting security compromises of the signaling networks supporting the public telephone network. This also applies to Public Safety in the context of transitional NG9-1-1 architectures involving Legacy Network Gateways and Legacy Selective Router Gateways.	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE
11-10-0731	Network Operators, Public Safety and Service Providers should provide physical diversity on critical inter-office and wireless backhaul routes when justified by a risk or value analysis.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0782	Network Operators, Public Safety and Service Providers should detect transport simplex events and restore the duplex protective path expeditiously by executing appropriate incident response and escalation processes.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0785	Network Operators, Public Safety and Service Providers should consider secured remote access to critical network management systems for network management personnel working from distributed locations (e.g., back-up facility, home) in the event of a situation where the NOC cannot be staffed (e.g., pandemic).	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-10-0787	Network Operators, Public Safety, Service Providers, and Property Managers should consider the use of fixed alternate fuel generators (e.g., natural gas) connected to public utility supplies to reduce the strain on refueling.	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0789	Network Operators, Public Safety, Service Providers, and Equipment Suppliers should consider modifying travel guidelines/policies for use during a pandemic or other crisis situations.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-0793	Network Operators, Public Safety, Service Providers, and Equipment Suppliers should, as part of business continuity planning, identify employees that can perform their tasks from alternate locations and consider provisions for enabling them to do so.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-0794	Network Operators, Public Safety, Service Providers, and Equipment Suppliers should, as part of business continuity planning, provide for elevated /increased utilization of remote access capabilities for telecommuting purposes by employees during a pandemic, or other crisis situations.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-0795	Network Operators, Public Safety, Service Providers, and Equipment Suppliers should as part of business continuity planning, plan for elevated/increased utilization of virtual collaboration and remote meetings capabilities during pandemics or other crisis situations.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-0796	Network Operators, Public Safety, Service Providers, and Equipment Suppliers should, as part of business continuity planning, consider developing guidelines for the deferral of specific maintenance or provisioning activities during certain situations (e.g., pandemic, holiday, National Special Security Event).	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-0806	Service Policies: Service Providers and Public Safety (for NG9-1-1) should establish policies and develop internal controls to ensure that the infrastructure supporting high speed broadband is protected from external threats, insider threats and threats from customers. These policies should cover protocol and port filtering as well as general security best practices.	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE
11-8-8001	Strong Encryption Algorithms and Keys: Service Providers, Network Operators, Public Safety (for NG9-1-1) and Equipment Suppliers should use industry-accepted algorithms and key lengths for all uses of encryption, such as 3DES or AES.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8007	Define Security Architecture(s): Service Providers, Public Safety and Network Operators should develop formal written Security Architecture(s) and make the architecture(s) readily accessible to systems administrators and security staff for use during threat response. The Security Architecture(s) should anticipate and be conducive to business continuity plans.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8011	Request OAM&P Security Features: Service Providers, Public Safety and Network Operators should request products from vendors that meet current industry baseline requirements for Operations, Administration, Management, and Provisioning (OAM&P) security.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8012	Secure Communications for OAM&P Traffic: To prevent unauthorized users from accessing Operations, Administration, Management, and Provisioning (OAM&P) systems, Service Providers, Public Safety and Network Operators should use strong authentication for all users. To protect against tampering, spoofing, eavesdropping, and session hijacking, Service Providers and Network Operators should use a trusted path for all important OAM&P communications between network elements, management systems, and OAM&P staff. Examples of trusted paths that might adequately protect the OAM&P communications include separate private-line networks, VPNs or encrypted tunnels. Any sensitive OAM&P traffic that is mixed with customer traffic should be encrypted. OAM&P communication via TFTP and Telnet is acceptable if the communication path is secured by the carrier. OAM&P traffic to customer premises equipment should also be via a trusted path.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8013	Controls for Operations, Administration, Management, and Provisioning (OAM&P) Management Actions: Service Providers, Public Safety and Network Operators should authenticate, authorize, attribute, and log all management actions on critical infrastructure elements and management systems. This especially applies to management actions involving security resources such as passwords, encryption keys, access control lists, time-out values, etc.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8014	OAM&P Privilege Levels: For OAM&P systems, Service Providers, Public Safety and Network Operators should use element and system features that provide "least-privilege" for each OAM&P user to accomplish required tasks using role-based access controls where possible.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8015	Segmenting Management Domains: For OAM&P activities and operations centers, Service Providers, Public Safety (for NG9-1-1) and Network Operators should segment administrative domains with devices such as firewalls that have restrictive rules for traffic in both directions and that require authentication for traversal. In particular, segment OAM&P networks from the Network Operator's or Service Provider's intranet and the Internet. Treat each domain as hostile to all other domains. Follow industry recommended firewall policies for protecting critical internal assets.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8016	OAM&P Security Architecture: Service Providers, Public Safety and Network Operators should design and deploy an Operations, Administration, Management, and Provisioning (OAM&P) security architecture based on industry recommendations.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8017	OAM&P Protocols: Service Providers, Network Operators, Public Safety (for NG9-1-1), and Equipment Suppliers should use Operations, Administration, Management and, Provisioning (OAM&P) protocols and their security features according to industry recommendations. Examples of protocols include SNMP, SOAP, XML, and CORBA.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8022	Remote Operations, Administration, Management and Provisioning (OAM&P) Access: Service Providers, Public Safety (for NG9-1-1) and Network Operators should have a process by which there is a risk assessment and formal approval for all external connections. All such connections should be individually identified and restricted by controls such as strong authentication, firewalls, limited methods of connection, and fine-grained access controls (e.g., granting access to only specified parts of an application). The remote party's access should be governed by contractual controls that ensure the provider's right to monitor access, defines appropriate use of the access, and calls for adherence to best practices by the remote party.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8040	Mitigate Control Plane Protocol Vulnerabilities: Service Providers, Public Safety (for NG9-1-1) and Network Operators should implement architectural designs to mitigate the fundamental vulnerabilities of many control plane protocols (eBGP, DHCP, SS7, DNS, SIP, etc.): 1) Know and validate who you are accepting information from, either by link layer controls or higher layer authentication, if the protocol lacks authentication, 2) Filter to only accept/propagate information that is reasonable/expected from that network element/peer.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8046	Protect DNS (Domain Name System) Servers Against Compromise: Service Providers, Public Safety (for NG91-1) and Network Operators should protect against DNS server compromise by implementing protection such as physical security, removing all unnecessary platform services, monitoring industry alert channels for vulnerability exposures, scanning DNS platforms for known vulnerabilities and security breaches, implementing intrusion detection on DNS home segments, not running the name server as root user/minimizing privileges where possible, and blocking the file system from being compromised by protecting the named directory.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8047	Protect Against DNS (Domain Name System) Denial of Service: Service Providers, Public Safety (for NG9-1-1) and Network Operators should provide DNS DoS protection by implementing protection techniques such as: 1) increase DNS resiliency through redundancy and robust network connections, 2) Have separate name servers for internal and external traffic as well as critical infrastructure, such as OAM&P and signaling/control networks, 3) Where feasible, separate proxy servers from authoritative name servers, 4) Protect DNS information by protecting master name servers with appropriately configured firewall/filtering rules, implement secondary masters for all name resolution, and using Bind ACLs to filter zone transfer requests.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8048	Protect DNS (Domain Name System) from Poisoning: Service Providers, Public Safety (for NG9-1-1), Network Operators, and Equipment Suppliers should mitigate the possibility of DNS cache poisoning by using techniques such as 1) Preventing recursive queries, 2) Configure short (2 day) Time-To-Live for cached data, 3) Periodically refresh or verify DNS name server configuration data and parent pointer records. Service Providers, Network Operators, and Equipment Suppliers should participate in forums to define an operational implementation of DNSSec.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8050	MPLS (Multi-Protocol Label Switching) Configuration Security: Service Providers, Public Safety (for NG9-1-1) and Network Operators should protect the MPLS router configuration by 1) Securing machines that control login, monitoring, authentication and logging to/from routing and monitoring devices, 2) Monitoring the integrity of customer specific router configuration provisioning, 3) Implementing (e)BGP filtering to protect against labeled-path poisoning from customers/peers.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8051	Network Access Control for SS7: Network Operators should ensure that SS7 signaling interface points that connect to the IP Private and Corporate networks interfaces are well hardened, protected with packet filtering firewalls; and enforce strong authentication. Similar safeguards should be implemented for e-commerce applications to the SS7 network. Likewise, Public Safety should implement such safeguards for transitional NG9-1-1 architectures that involve Legacy Network Gateways and Legacy Selective Router Gateways. Network Operators should implement rigorous screening on both internal and interconnecting signaling links and should investigate new, and more thorough screening capabilities. Operators of products built on general purpose computing products should proactively monitor all security issues associated with those products and promptly apply security fixes, as necessary. Operators and Public Safety should be particularly vigilant with respect to signaling traffic delivered or carried over Internet Protocol networks. Network Operators that do employ the Public Internet for signaling, transport, or maintenance communications and any maintenance access to Network Elements should employ authentication, authorization, accountability, integrity, and confidentiality mechanisms (e.g., digital signature and encrypted VPN tunneling).	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8052	SS7 Authentication: Network Operators should mitigate limited SS7 authentication by enabling logging for SS7 element security related alarms on SCPs and STPs, such as: unauthorized dial up access, unauthorized logins, logging of changes and administrative access logging. Network operators should implement rigorous screening on both internal and interconnecting signaling links and should investigate new and more thorough screening capabilities. Likewise, Public Safety should enable logging for SS7 element security-related alarms on Legacy Network Gateways and Legacy Selective Routing Gateways for transitional NG9-1-1 architectures. Operators of products built on general purpose computing products should proactively monitor all security issues associated with those products and promptly apply security fixes, as necessary. Operators and Public Safety should establish login and access controls that establish accountability for changes to node translations and configuration. Operators and Public Safety (for NG9-1-1) should be particularly vigilant with respect to signaling traffic delivered or carried over Internet Protocol networks. Network operators that do employ the Public Internet for signaling, transport or maintenance communications and any maintenance access to Network Elements shall employ authentication, authorization, accountability, integrity and confidentiality mechanisms (e.g. digital signature and encrypted VPN tunneling). Operators and Public Safety making use of dial-up connections for maintenance access to Network Elements should employ dial-back modems with screening lists. One-time tokens and encrypted payload VPNs should be the minimum.	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE
11-8-8075	Identity Administration: Network Operators, Public Safety and Service Providers should have procedures for verifying identity of users to IT department and IT personnel to users (secret PINs, callback procedures, etc.).	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8085	Expiration of Digital Certificates: Service Providers, Public Safety (for NG9-1-1), Network Operators, and Equipment Suppliers, certificates should have a limited period of validity, dependent upon the risk to the system, and the value of the asset. If there are existing certificates with unlimited validity periods, and it is impractical to replace certificates, consider the addition of passwords that are required to be changed on a periodic basis.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8087	Use Time-Specific Access Restrictions: Service Providers, Public Safety and Network Operators should restrict access to specific time periods for high risk users (e.g., vendors, contractors, etc.) for critical assets (e.g., systems that cannot be accessed outside of specified maintenance windows due to the impact on the business). Assure that all system clocks are synchronized.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8088	Develop Regular Access Audit Procedures: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should charter an independent group (outside of the administrators of the devices) to perform regular audits of access and privileges to systems, networks, and applications. The frequency of these audits should depend on the criticality or sensitivity of the associated assets.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8097	Create Policy on Information Dissemination: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should create an enforceable policy clearly defining who can disseminate information, and what controls should be in place for the dissemination of such information. The policy should differentiate according to the sensitivity or criticality of the information.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8098	Create Policy on Removal of Access Privileges: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should have policies on changes to and removal of access privileges upon staff members status changes such as terminations, exits, transfers, and those related to discipline or marginal performance.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8099	Create Policy on Personnel Hiring Merits: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should perform background checks that are consistent with the sensitivity of the position's responsibilities and that align with HR policy. These checks could include those that verify employment history, education, experience, certification, and criminal history.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8100	Training for Security Staff: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should establish security training programs and requirements for ensuring security staff knowledge and compliance. This training could include professional certifications in cyber security.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8108	Authentication System Failure: In the event of an authentication system failure, Service Providers, Public Safety and Network Operators should determine how the system requiring support of the authentication system responds (i.e., determine what specific effect(s) the failure caused). The system can either be set to open or closed in the event of a failure. This will depend on the needs of the organization. For instance, an authentication system supporting physical access may be required to fail OPEN in the event of a failure, so people will not be trapped in the event of an emergency. However, an authentication system that supports electronic access to core routers may be required to fail CLOSED to prevent general access to the routers in the event of authentication system failure. In addition, it is important to have a means of alternate authenticated access to a system in the event of a failure. In the case of core routers failing CLOSED, there should be a secondary means of authentication (e.g., use of a one-time password) reserved for use only in such an event; this password should be protected and only accessible to a small key-contingent of personnel.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8112	Protect Management of Externally Accessible Systems: Service Providers, Public Safety (for NG9-1-1) and Network Operators should protect the systems configuration information and management interfaces for Web servers and other externally accessible applications, so that it is not inadvertently made available to 3rd parties. Techniques, at a minimum, should include least privilege for external access, strong authentication, application platform hardening, and system auditing.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8117	DNS Servers Disaster Recovery Plan: Service Providers, Public Safety (for NG9-1-1) and Network Operators should prepare a disaster recovery plan to implement upon DNS server compromise.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8118	Protect Against DNS (Domain Name System) Distributed Denial of Service: Service Providers, Public Safety (for NG9-1-1) and Network Operators should provide DNS DDoS protection by implementing protection techniques such as: 1) Rate limiting DNS network connections 2) Provide robust DNS capacity in excess of maximum network connection traffic 3) Have traffic anomaly detection and response capability 4) Provide secondary DNS for back-up 5) Deploy Intrusion Prevention System in front of DNS.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8119	Security-Related Data Correlation: Service Providers, Public Safety (for NG9-1-1) and Network Operators should correlate data from various sources, including non-security related sources, (i.e., syslogs, firewall logs, IDS alerts, remote access logs, asset management databases, human resources information, physical access logs, etc.) to identify security risks and issues across the enterprise.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8125	Policy Acknowledgement: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should ensure that employees formally acknowledge their obligation to comply with their corporate/agency Information Security policies.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8126	Use Risk-Appropriate Authentication Methods: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should employ authentication methods commensurate with the business risk of unauthorized access to the given network, application, or system. For example, these methods would range from single-factor authentication (e.g., passwords) to two-factor authentication (e.g., token and PIN) depending on the estimated criticality or sensitivity of the protected assets. When two-factor authentication generates one-time passwords, the valid time-duration should be determined based on an assessment of risk to the protected asset(s).	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8127	Verify Audit Results Through Spot-Checking: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should validate any regular auditing activity through spot-checking to validate the competency, thoroughness, and credibility of those regular audits.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8128	Promptly Address Audit Findings: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should promptly verify and address audit findings assigning an urgency and priority commensurate with their implied risk to the business. The findings as well as regular updates to those findings should be reported to management responsible for the affected area.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8129	Staff Training on Technical Products and Their Controls: To remain current with the various security controls employed by different technologies, Service Providers, Public Safety, Network Operators, and Equipment Suppliers should ensure that technical staff participate in ongoing training and remain up-to-date on their certifications for those technologies.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8130	Staff Trained on Incident Reporting: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should provide procedures and training to staff on the reporting of security incidents, weaknesses, and suspicious events.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8138	Renewal of Digital Certificates: Service Providers, Public Safety (for NG9-1-1), Network Operators, and Equipment Suppliers should establish a procedure to track the expiration date for digital certificates used in services and critical applications, and start the process to renew such certificates in sufficient time to prevent disruption of service.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8500	Recovery from Digital Certificate Key Compromise: In the event the key in a digital certificate becomes compromised, Service Providers, Public Safety (for NG9-1-1), Network Operators, and Equipment Suppliers should immediately revoke the certificate, and issue a new one to the users and/or devices requiring it. Perform Forensics and Post-mortem, as prescribed in NRIC BP 8061, to review for additional compromise as soon as business processes allow.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8501	Recovery from Root Key Compromise: In the event the root key in a digital certificate becomes compromised, Service Providers, Public Safety (for NG9-1-1), Network Operators, and Equipment Providers should secure a new root key, and rebuild the PKI (Public Key Infrastructure) trust model. Perform Forensics and Post-mortem, as prescribed in NRIC BP 8061, to review for additional compromise as soon as business processes allow.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8503	Recovery from Encryption Key Compromise or Algorithm Failure. When improper use of keys or encryption algorithms is discovered, or a breach has occurred, Service Providers, Public Safety (for NG9-1-1), and Network Operators should conduct a forensic analysis to assess the possibility of having potentially compromised data and identify what may have been compromised and for how long it has been in a compromised state; implement new key (and revoke old key if applicable), or encryption algorithm, and ensure they are standards-based and implemented in accordance with prescribed procedures of that standard, where possible. When using wireless systems, ensure vulnerabilities are mitigated with proper and current security measures.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8517	Recovery from Unauthorized Information Dissemination: If information has been leaked or the release policy has not been followed, Service Providers, Public Safety, Network Operators, and Equipment Suppliers should review audit trails; Change passwords, review permissions, and perform forensics as needed; Inform others at potential risk for similar exposure; and include security responsibilities in performance improvement programs that may include security awareness refresher training.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8527	Recover from Compromised DNS (Domain Name System) Servers or Name Record Corruption: If the DNS (Domain Name System) server has been compromised or the name records corrupted, Service Providers, Public Safety (for NG9-1-1) and Network Operators should first flush the DNS cache and, failing that, implement the pre-defined disaster recovery plan. Elements may include but are not limited to: 1) bring-on additional hot or cold spare capacity, 2) bring up a known good DNS server from scratch on different hardware, 3) Reload and reboot machine to a known good DNS server software (from bootable CD or spare hard drive), 4) Reload name resolution records from a trusted back-up. After the DNS is again working, conduct a post-mortem of the attack/response.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8528	Recover from DNS (Domain Name Server) Denial of Service Attack: If the DNS server is under attack, Service Providers, Public Safety (for NG9-1-1) and Network Operators should consider one or more of the following steps 1) Implement reactive filtering to discard identified attack traffic, if possible, 2) Rate-limiting traffic to the DNS server complex, 3) Deploy suitable Intrusion Prevention System in front of DNS servers, 4) Deploy additional DNS server capacity in a round-robin architecture, 5) Utilize DoS/DDoS tracking methods to identify the source(s) of the attack, or 6) Move name resolution service to a 3rd party provider.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8561	Recovery from Denial of Service Attack - Target: If a network element or server is under DoS attack, Service Providers, Public Safety (for NG9-1-1) and Network Operators should evaluate the network and ensure issue is not related to a configuration/hardware issue. Determine direction of traffic and work with distant end to stop inbound traffic. Consider adding more local capacity (bandwidth or servers) to the attacked service. Where available, deploy DoS/DDoS specific mitigation devices and/or use anti-DoS capabilities in local hardware. Coordinate with HW vendors for guidance on optimal device configuration. Where possible, capture hostile code and make available to organizations such as US-CERT and NCS/NCC for review.	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8633	Wireless Policies and Standards: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should design passwords used for an application login to be consistent with applicable industry security guidelines and policies. Whether between the client and the server or among servers, passwords must not be transmitted "in the clear." SSL should be used for any transaction involving authentication. The transmission of session IDs should be similarly protected with SSL.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8642	Wireless Standards: Service Providers, Public Safety and Network Operators should consider integration of open standardized protocols to meet communication-level performance and security goals.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8652	General: Service Provider, Public Safety and Network Operators should implement access controls (firewalls, access control lists, etc.) to administrative interfaces as well as those normally carrying customer traffic.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8653	General: Service Providers, Public Safety (for NG9-1-1) and Network Operators should test current equipment for IPv4/IPv6 compatibility for the specific network deployment.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8670	Protect exchange of information: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should consider establishing information exchange policies and procedures, establish information and software exchange agreements, safeguard transportation of physical media.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8671	Protect Unattended Workstations: Service Providers, Public Safety, and Network Operators should have policies and enforce that unattended workstations should be protected from unauthorized access 1) Individual Username/Password authentication must be required to access resources. 2) Physical access must be restricted to workstations. 3) Where possible idle workstations must default to password protected screensaver after an established time lapse (e.g. 15 minutes).	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8693	Cybersecurity Awareness: Network Operators, Public Safety, Service Providers and Equipment Suppliers should create a security awareness strategy that includes communicating to everyone from new hires to human resources to senior management. Utilize multiple channels and target each audience specifically.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8694	Threat Management: Network Operators, Public Safety, Service Providers and Equipment Suppliers should keep their programs flexible. What is considered a security best practice today might be obsolete tomorrow. Changing factors include new technologies, changing business models, emerging threats and growth of the network and the user base.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8695	Management Support: Network Operators, Public Safety, Service Providers and Equipment Suppliers should obtain senior management approval and support for a corporate wide People/Awareness/Security Awareness program. This will help to lead to behavior and policy changes.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8701	Security Maturity and Metrics: Network Operators, Service Providers, Public Safety and Equipment Suppliers should measure the effectiveness of their Security programs.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8703	Security Policy: Network Operators, Service Providers, Public Safety and Equipment Suppliers should establish and enforce policy to lock up paperwork and magnetic media containing confidential information and destroy it when it is no longer needed.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8704	Security Policy: Network Operators, Service Providers, Public Safety and Equipment Suppliers should establish and enforce policy to physically secure the computers and network devices.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-8-8705	Identity Administration: Network Operators, Public Safety and Service Providers should have procedures for verifying identity of users to IT department and IT personnel to users (secret PINs, callback procedures, etc.).	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8706	Identity Administration: Network Operators, Public Safety and Service Providers should establish and enforce policy to prohibit disclosing passwords, to whom (if anyone) passwords can be disclosed and under what circumstances, procedure to follow if someone requests disclosure of passwords.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8711	Media Gateway Availability: Network Operators, Public Safety (for NG9-1-1) and Service Providers should engineer networks to provide redundant and highly available application layer services. (e.g., DNS and other directory services, SIP, H.323).	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8712	Media Gateway Interoperability: Network Operators, Public Safety (for NG9-1-1) and Service Providers should implement applicable industry standards governing protocol (e.g., IP Protocols from the IETF) and established policies and procedures to maintain currency within these publications to ensure interoperability.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8722	Signaling Over Public IP: Network Operators and Public Safety (for NG9-1-1) should be particularly vigilant with respect to signaling traffic delivered by or carried over Internet Protocol networks. Network Operators that utilize the Public Internet for signaling, transport, or maintenance communications should employ authentication, authorization, accountability, integrity, and confidentiality mechanisms (e.g., digital signature and encrypted VPN tunneling).	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE
11-8-8728	Maintaining Logical Link Diversity: Network Operators and Public Safety (for NG9-1-1) who deploy next generation signaling networks should consider industry guidelines for logical diversity (e.g. multi-homing), and perform network diversification validation on a scheduled basis (e.g., twice a year). Processes and procedures should exist for tracking discrepancies and maintaining a historical record.	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE
11-8-8732	"General: Service Providers and Public Safety (for NG9-1-1) should classify identity management services against the service architecture and deployment model being utilized to determine the general "security" posture of the identity services, how it relates to asset's assurance and security protection requirements, and define the needed security architecture to mitigate security risks. Specifically, if identity related functions are distributed among multiple parties, all parties involved should be clearly identified (e.g., relying parties such as users and service providers, credential providers, verifier or authentication providers, or federation members) with clearly defined roles, responsibilities, and accountability for the security of the identity service and all associated assets."	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8734	Identity Data Security – Service providers and Public Safety (for NG9-1-1) creating, maintaining, using or disseminating individually identifiable information should take appropriate measures to assure its reliability and should take reasonable precautions to protect it from loss, misuse or alteration. Organizations/Agencies should take reasonable steps to assure that third parties to which they transfer such information are aware of these security practices, and that the third parties also take reasonable precautions to protect any transferred information.	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE
11-8-8736	Identity Information Access Control: Service Providers and Public Safety should ensure that identity information is only accessible to authorized entities subject to applicable regulation and policy. Specifically, (a) an entity (e.g., relying party or requesting party) requesting identity data should be authenticated, and its authorization to obtain the requested information verified before access to the information is provided or the requesting identity data is exchanged. (b) policy and rules for requesting and exchanging identity data among multiple parties involved (e.g., users, relying party and identity provider) should be clearly defined and enforced.	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE
11-8-8737	SAML Privacy: Service Providers and Public Safety (for NG9-1-1) should analyze each of the steps in the interaction (and any subsequent uses of data obtained from the transactions) of a Security Assertion Markup Language (SAML) transaction to ensure that information that should be kept confidential is actually being kept so.	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE
11-8-8742	General: Service Providers and Public Safety (for NG9-1-1) should use encryption for data at rest.	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE
11-8-8749	Risk Assessment Process: Service providers, Public Safety and network operators should have documented processes in place for reviewing new vulnerabilities as they are announced.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-8-8758	Post DoS Practice: Network Operators, Public Safety (for NG9-1-1) and Service Providers should establish policies, and procedures to support early recognition and isolation of potential bad actors to minimize impact to the network.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-8-8770	SAML Communications: Service Providers and Public Safety (for NG9-1-1) should use secure network protocols such as TLS or IPsec to provide integrity and confidentiality protection of SAML communications. In addition, the following measures should be implemented to counter replay, denial of service and other forms of attacks: (a) Clients should be required to authenticate at some level below the SAML protocol level (for example, using the SOAP over HTTP binding, with HTTP over TLS/SSL, and with a requirement for client-side certificates that have a trusted Certificate Authority at their root) to provide traceability and counter DOS attacks. (b) Use of the XML Signature element [ds:SignatureProperties] containing a timestamp should be required to determine if a signature is recent to counter replay attacks. (c) Maintaining state information concerning active sessions, and validate correspondence. (d) Correlation of request and response messages.	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE
11-9-0519	Capacity Monitoring: Network Operators, Public Safety (for NG9-1-1) and Service Providers should engineer and monitor networks to ensure that operating parameters are within capacity limits of their network design (e.g., respect limitations of deployed packet switches, routers and interconnects, including "managed networks" and "managed CPE"). These resource requirements should be re-evaluated as services change or grow.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0529	Network Operators, Service Providers, Public Safety and Equipment Suppliers should support sharing of appropriate information pertaining to outages as an effort to decrease the potential of further propagation.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-0592	Network Operators, Public Safety (for NG9-1-1) and Service Providers should provide duplicated, non-co-located maintenance administration, surveillance and support for network elements.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0596	Network Operators, Public Safety and Service Providers should carefully review all re-home procedures, undertake pre-planning before execution, and ensure that re-home procedures (e.g. support interconnection to ESInets during transition), are carefully followed.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-10-0602	Network Operators, Public Safety and Service Providers should establish procedures to reactivate alarms after provisioning or maintenance activities (when alarms are typically deactivated).	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0608	Network Operators, Public Safety and Service Providers including OSPs and E9-1-1/NG9-1-1 SSPs should utilize network surveillance and monitoring to keep overflow traffic conditions from adversely affecting networks.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-10-0612	Network Operators, Public Safety and Service Providers should verify both local and remote alarms and remote network element maintenance access on all new critical equipment installed in the network, before it is placed into service.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-9-0616	Network Operators, Public Safety and Service Providers should design and implement procedures to evaluate failure and emergency conditions affecting network capacity.	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE
11-10-0630	Network Operators, Service Providers, Equipment Suppliers, Public Safety and Property Managers should develop and execute standard Methods of Procedure (MOP) for all vendor work in or external to equipment locations with emphasis on service continuity and safety precautions.	TRUE	TRUE	FALSE	TRUE	TRUE	TRUE
11-10-0693	Network Operators, Service Providers, Public Safety and Property Managers should emphasize the use of Methods Of Procedures (MOPs), vendor monitoring, and performing work on in-service equipment during low traffic periods (i.e., maintenance window).	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE
11-9-0762	Network Operators should engineer networks supporting VoIP applications (including access to NG9-1-1 NGCS) to provide redundant and highly available application layer services.	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE
11-9-1063	Network Operators and Service Providers should set Initial Address Messages (IAMs) to congestion priority in accordance with applicable ANSI standards. This will ensure government emergency calls (e.g., 9-1-1, GETS) receive proper priority during national emergency situations. Implementation in all networks should be in accordance with ANSI T1.111.	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-9-3205	Network Operators, Service Providers and Public Safety organizations should consider participating in standards bodies and other forums contributing to Emergency Telecommunications Services (ETS) and NG9-1-1 related standards development.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-9-3214	Public Safety should support automated location query capability including rebids, but avoid the sending of overlapping location queries that would negatively impact current location determination capabilities.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-11-3215	Wireless Service Providers and Network Operators, in the absence of better routing information, should route 9-1-1 calls based on cell sector/tower location toward the designated serving Public Safety Answering Point (PSAP) via the Emergency Service Network when necessary and where feasible.	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
11-9-3216	For Network Operators that cannot route 9-1-1 calls based on cell sector/tower location, switch level defaulted calls should be routed to a "fast busy" treatment, or to a dedicated call center, or to an appropriate recorded announcement.	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
11-9-3218	Public Safety should provide Training to educate PSAP personnel as to the process to obtain 9-1-1 Phase II data.	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
11-9-3219	Public Safety should provide training to educate PSAP personnel as to the proper meaning and interpretation of the E9-1-1 Phase II display parameters.	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
11-11-3223	Network Operators, Public Safety and Service Providers should implement dedicated and as diverse trunk groups as feasible and commercially reasonable as possible between the Mobile Switching Center (MSC) end office or similar source and the E9-1-1 Selective Router (SR) or Legacy Network Gateway (for NG9-1-1), based on the geography served by the default Public Safety Answering Points (PSAPs).	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-11-3224	Network Operators, Service Providers, and Public Safety should use dedicated and diverse Signaling System 7 (SS7) or Multi-Frequency (MF) controlled trunk groups as feasible and commercially reasonable as possible for the normal routing of 9-1-1 calls from originating switching entities to 9-1-1 Selective Routers (SRs) or Legacy Network Gateway (for NG9-1-1) rather than using shared Public Switched Telephone Network (PSTN) trunk arrangements and where appropriate and necessary supported by service level agreements. Network Operators, Service Providers, and NG9-1-1 PSAPs should use dedicated, geo-diverse and redundant IP connection points when feasible & commercially available.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-9-3225	Network Operators, Public Safety and Service Providers that deploy geographically diverse 9-1-1 location servers with dual load sharing nodes should ensure that the utilization on either node is less than half of each node's capacity so that if one node fails the other node will absorb the load.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-9-3226	Network Operators, Public Safety and Service Providers should provide 24x7 network operations support.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-9-3227	Network Operators, Service Providers, Public Safety and Equipment Suppliers should deploy location solutions such that the 9-1-1 related data traffic between the Network Operator's location server and the mobile device should not degrade voice quality.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-9-3229	Network Operators, Public Safety and Service Providers should maintain all 9-1-1 call data according to all applicable governmental data retention requirements. In the absence of governmental data retention requirements, the call data should be retained in accordance with FCC guidelines.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-9-3230	Network Operators, Public Safety and Service Providers that produce location event records that include time-stamped call detail transactions should maintain such records according to all applicable governmental data retention requirements. In the absence of governmental data retention requirements, the call data should be retained in accordance with FCC guidelines.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-9-3231	Network Operators, and Service Providers that use Global Positioning System (GPS) enabled Phase II location solutions should ensure that the GPS satellite location identification information (e.g., GPS ephemeris, almanac, etc.) is transmitted to the Phase II Mobile Subscriber or Position Determining Entities (PDE) as soon as is feasible after the 9-1-1 call commences in order to reduce the number of database query rebids.	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-9-3234	Network Operators, Service Providers, and Public Safety should use Policy-based Routing and/or other tactical routing functionality defined for Next Generation 9-1-1 (NG9-1-1) to handle call congestion and outages through diversion of calls to alternate Public Safety Answering Points (PSAP) that have the capabilities to effectively answer and provide assistance during periods of extreme overload or network failure scenarios.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-9-5112	Network Operators, Service Providers, Public Safety and Equipment Suppliers should, at the time of the abnormal event, coordinate with the appropriate local, state, or federal agencies to facilitate timely access by their personnel to establish, restore or maintain communications, through any governmental security perimeters (e.g., civil disorder, crime scene, disaster area).	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE
11-9-5132	Network Operators and Public Safety should identify primary and alternate transportation (e.g., air, rail, highway, boat) for emergency mobile units and other equipment and personnel.	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE
11-9-5175	Network Operators, Service Providers, Public Safety and Equipment Suppliers should establish a proprietary information protection policy to protect proprietary information in their possession belonging to the company/agency, business partners and customers from inadvertent, improper or unlawful disclosure. The policy should establish procedures for the classification and marking of information; storage, handling, transfer and transmission of information, retention guidelines and disposal/deletion of information.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-9-5241	Network Operators, Service Providers, Pubic Safety and Equipment Suppliers should consider placing access and facility alarm points to critical or sensitive areas on backup power to ensure access and functionality during periods of power outages.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-9-5260	Network Operators, Service Providers, Equipment Suppliers, Pubic Safety and Property Managers should provide personnel involved in a restoration any significant changes to access control procedures.	TRUE	TRUE	FALSE	TRUE	TRUE	TRUE
11-9-8005	Document Single Points of Failure: Service Providers, Public Safety and Network Operators should implement a continuous engineering process to identify and record single points of failure and any components that are critical to the continuity of the infrastructure. The process should then pursue architectural solutions to mitigate the identified risks as appropriate.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-9-8026	Distribution of Encryption Keys: When Service Providers, Public Safety, Network Operators, and Equipment Suppliers use an encryption technology in the securing of network equipment and transmission facilities, cryptographic keys must be distributed using a secure protocol that: a) Ensures the authenticity of the sender and recipient, b) Does not depend upon secure transmission facilities, and c) Cannot be emulated by a non-trusted source.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-9-8071	Threat Awareness: Service providers, Public Safety and Network Operators should subscribe to vendor patch/security notifications and services to remain current with new vulnerabilities, viruses, and other security flaws relevant to systems deployed on the network.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-9-8079	Use Strong Passwords: Service Provider, Public Safety, Network Operators, and Equipment Suppliers should create an enforceable policy that considers different types of users and requires the use of passwords or stronger authentication methods. Where passwords can be used to enhance needed access controls, ensure they are sufficiently long and complex to defy brute force guessing and deter password cracking. To assure compliance, perform regular audits of passwords on at least a sampling of the systems.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-9-8080	Change Passwords on a Periodic Basis: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should change passwords on a periodic basis implementing a policy which considers different types of users and how often passwords should be changed. Perform regular audits on passwords, including privileged passwords, on system and network devices. If available, activate features across the user base which force password changes.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-9-8081	Protect Authentication Methods: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should develop an enforceable password policy, which considers different types of users, requiring users to protect, as applicable, either (a) the passwords they are given/create or (b) their credentials for two-factor authentication.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-9-8101	Document and Verify All Security Operational Procedures: Service Providers, Public Safety and Network Operators should ensure that all security operational procedures, system processes, and security controls are documented, and that documentation is up to date and accessible by appropriate staff. Perform gap analysis/audit of security operational procedures as often as security policy requires relative to the asset being protected. Using results of analysis or audit, determine which procedures, processes, or controls need to be updated and documented.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-9-8111	Protect Sensitive Data in Transit for Externally Accessible Applications: Service Providers, Public Safety (for NG9-1-1) and Network Operators should encrypt sensitive data from web servers, and other externally accessible applications, while it is in transit over any networks, they do not physically control.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-9-8124	Conduct Organization Wide Security Awareness Training: Service Providers, Public Safety, Network Operators, and Equipment Suppliers should ensure staff is given awareness training on security policies, standards, procedures, and general best practices. Awareness training should also cover the threats to the confidentiality, integrity, and availability of data including social engineering. Training as part of new employee orientation should be supplemented with regular "refreshers" to all staff.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
11-9-8540	Recover from Unauthorized Remote OAM&P Access: When an unauthorized remote access to an OAM&P system occurs, Service Providers, Public Safety and Network Operators should consider terminating all current remote access, limiting access to the system console, or other tightened security access methods. Continue recovery by re-establishing new passwords, reloading software, running change detection software, or other methods, continuing quarantine until recovery is validated, as practical.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

OLD BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
11-9-8771	Service Providers, Network Operators, and Public Safety should implement media gateway controllers according to appropriate industry standards (i.e. Internet Engineering Task Force (IETF), Alliance for Telecommunications Industry Solutions (ATIS)) in order to achieve interoperability between the IP Multimedia (IM) Core Network (CN) subsystem and Legacy Emergency Services networks.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-11-3245	Network Operators, Service Providers, and Public Safety should develop policy routing procedures that consider the full capability of NG9-1-1, including the rerouting of calls from other PSAPs as a result of overflow, backup, and disaster situations. Inter-agency agreements should be updated to reflect the updated procedures.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11-11-3246	Network Operators, where MSC capabilities exist should route calls based on the location of the cell tower, to the MSC-SR trunks designated for that cell site to the serving PSAP. Switch level defaulted calls shall be routed to a "fast busy" tone or, where that option is not available, to an appropriate recorded announcement.	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
11-11-3247	Public Safety should conduct on-going meetings with several bordering or nearby PSAPs to clarify the wireless 9-1-1 call routing determination process. For example, it may be appropriate to route a cell site/sector based on the area covered or where the highest density population exists.	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
11-11-3248	Public Safety should obtain GIS data from bordering PSAP jurisdictions and expanding and testing their transfer list to bordering PSAPs. This is necessary as the routing of wireless 9-1-1 calls may require a PSAP to receive and transfer calls for an area larger than the wireline coverage area.	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE

17 Appendix C –Recommended NEW 9-1-1 Related Best Practices.

Based upon the Working Group analysis, the proposed Best Practices in this Appendix are recommended to be incorporated in the FCC Best Practice database. While the Working Group was focused on NG9-1-1 and the transition to it, the Working Group took the liberty to define some Best Practices that were more general in nature.

NEW BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
1	Interconnecting networks should have their physical POIs for signaling and media documented in an Interconnection Agreement. Specifically, for NG9-1-1, unless local requirements differ, those POI should be at the ingress Border Control Function (BCF) of the ESInet.	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
2	Interconnecting networks should have their physical POIs for NG9-1-1 dereferencing functions documented in an Interconnection Agreement. Specifically, for NG9-1-1, unless local requirements differ, those POI should be at the ingress Firewall of the ESInet or NG9-1-1 PSAP.	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
3	Network Operators and Service Providers should address the control of overflow conditions in their bilateral agreements with their interconnection partners.	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE
4	Network Operators, Public Safety and Service Providers should coordinate DOS and TDOS detection, verification and recovery efforts with local law enforcement, cybersecurity task forces, State Threat Assessment centers and other law enforcement agencies. The PSAP should have procedures in place that minimize the impact of DOS and TDOS while preserving the evidence needed to support the investigation.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
5	Spam: Network Operators, Service Providers, and Public Safety should apply caller authentication/verification techniques (e.g., using the SHAKEN framework) to mitigate Caller ID spoofing.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

NEW BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
6	Network Operators, Service Providers, and Public Safety should strive to ensure that locations associated with 9-1-1 calls are validated in the OSP network (if in civic format), correctly determined, and successfully conveyed to support the routing of emergency calls by the NG9-1-1 system, and the delivery of caller location to Public Safety Answering Points.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
7	Network Operators, Service Providers and Public Safety should assess the impact on the routing and delivery of 9-1-1 calls and associated data to legacy and NG PSAPs associated with configuring their networks to support IP connections to NG PSAPs, Legacy Selective Router Gateways, and Legacy PSAP Gateways, as well as SS7-supported trunk connections between Legacy Selective Router Gateways and legacy Selective Routers, and MF trunks from Legacy PSAP Gateways and legacy Selective Routers to legacy PSAPs.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
8	Network Operators, Service providers, and Public Safety should be able to access logging data via a standard interface, with proper authorization.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
9	Network Operators and Service Providers routing 911 calls via an NG9-1-1 Emergency Services Networks from conventional TDM-based originating networks should consider using Legacy Network Gateways that support standards-based mappings of MF/SS7 signaling to SIP messages should also support (at a minimum) G.711 codecs, in order to achieve consistent signaling interworking and to support voice band communication industry-wide.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
10	Network Operators and Service Providers routing 911 calls to legacy PSAPs via an NG9-1-1 Emergency Services Network should consider using Legacy PSAP Gateways that support standards-based mappings of SIP messaging to MF signaling, or Legacy Selective Router Gateways that support standards-based mappings of SIP messaging to SS7 signaling in order to achieve consistent interworking industry-wide.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
11	Spam: Network Operators, Service Providers, and Public Safety should enforce authentication of NGCS functional elements and PSAP agents/agencies prior to granting access to NG9-1-1/ESInet services and data.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

NEW BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
12	9-1-1 Network Operators, Service Providers and Public Safety should assess the impact on the routing and delivery of 9-1-1 calls and associated data to legacy and NG PSAPs associated with configuring their networks. This may include IP connections from NG9-1-1 Emergency Services Networks to NG PSAPs, Legacy Selective Router Gateways, and Legacy PSAP Gateways; SS7-supported trunk connections between Legacy Selective Router Gateways and legacy Selective Routers; and MF trunks from Legacy PSAP Gateways and legacy Selective Routers to legacy PSAPs.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
13	Operators of NG9-1-1 Emergency Services Networks, Service Providers, and Public Safety should support access to a logging service (also referred to as a "logger") by all Next Generation Core Services (NGCS) elements and NG PSAPs that are served by an i3 NG9-1-1 Emergency Services IP Network (ESInet) via a standard interface. All significant steps in processing a call should logged, including external events, internal events, media, and messages. Access to at least two loggers must be supported for redundancy purposes, unless jurisdictional requirements differ.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
14	Network Operators, Service Providers, and Public Safety entities who support transitional NG9-1-1 architectures and are responsible for operating Legacy Network Gateways, Legacy PSAP Gateways, and/or Legacy Selective Router Gateways should ensure that these gateway elements log the beginning (i.e., start time) and end of processing (i.e., end time) of a call, as well as the actual SIP message processed by the gateway element via its IP interface and data related to its legacy interface (e.g., the port or trunk group over which the call was received/sent, the 10-digit pANI received or generated by the gateway system, the legacy protocol used [SS7 or MF]), in accordance with NENA requirements.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
15	Network Operators, Public Safety and Service Providers should implement policy routing rules for NG9-1-1 that allow 911 calls to be alternate routed to another PSAP due to an abnormal condition at the original PSAP, e.g., PSAP shutdown, abandonment, etc. The PSAP should be responsible for defining these conditions and have access to invoke them.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
16	Network Providers, Service Providers and Public Safety (for NG9-1-1) should use secure network protocols such as TLS for network interconnection for their SIP traffic.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
17	Network Operators, Public Safety, Property Managers and Service Providers should protect their building facilities against external breaches (e.g., vehicles inadvertently or purposefully ramming into the data center, NOC, operations center, etc.).	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE

NEW BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
18	Network Operators, Public Safety and Service Providers should identify and manage critical network elements and architecture that are essential for network connectivity and subscriber services considering security, functional redundancy and geographical diversity.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
19	Network Operators, Public Safety and Service Providers should, where feasible, provide both physical and logical diversity of critical facilities links.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
20	Operators of NG9-1-1 Emergency Services Networks, Service Providers, and Public Safety operators of NG PSAP networks should support Border Control Functions (BCFs) that provide border firewall functionality including application and network layer protection and scanning, resource and admission control, and Denial of Service (DoS) detection and protection, as well as Session Border Control (SBC) functionality including: identification of emergency call/session and priority handling for the IP flows of emergency call/session traffic; conformance checking and mapping (if applicable) of priority marking based on policy for emergency calls/sessions; SIP protocol normalization; Network Address Translation (NAT) and Network Address and Port Translation (NAPT) Traversal; IPv4/IPv6 Interworking; Signaling Transport Protocol Support; and QoS/Priority Packet Marking.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
21	Authentication for NG9-1-1: Service Providers and Network Operators (for NG9-1-1) should use strong certificate-based authentication ensuring network access, digital content and software services can be secured from unauthorized access. All protocol operations should be integrity-protected with TLS, using SHA 256 or stronger.	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE
22	Network Operators, Service Providers and Public Safety should establish and enforce policies that ensure cloud based Next Gen 9-1-1 services provide resilience, performance and security that meet established best practices for public safety and 9-1-1 and that leverage the scalable and enhanced information technology capacities of cloud based Next Gen 9-1-1 services.	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE
23	Network Operators, Service Providers and Public Safety for NG9-1-1 should provide integrity protection with TLS using SHA-256 or stronger.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

NEW BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
24	Originating Service Providers, NG9-1-1 System Service Providers, Network Operators, and Public Safety should support HTTPS transport of dereference requests associated with the acquisition of location information and other additional data associated with an emergency call.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
25	Network Operators, Service Providers and Public Safety should establish and enforce policies for log in requirements, password protection, screen lock upon activity timeout, and other physical security measures to prevent visitors and outside contractors from accessing NG9-1-1 systems.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
26	Identity Administration: Network Operators, Service Providers and Public Safety should establish policies governing data, metadata, and other media that hold information that could be used to compromise the security in an NG9-1-1 system.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
27	Vulnerability Assessment, Reporting & Remediation: Public Safety, Service Providers, Network Operators, and Equipment Suppliers should consider the use of the Department of Homeland Security (DHS) Protected Critical Infrastructure Information (PCII) program as a means of aggregating, sharing and protecting Vulnerability Assessment, Reporting & Remediation information related to private sector infrastructure. Program information can be found at https://www.dhs.gov/pcii-program.	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
28	Network Operators, NG9-1-1 System Service Providers, and Public Safety should support redundant local DNS servers/resolvers for any element connected to an NG9-1-1 Emergency Services IP Network to support the translation of hostnames to IP addresses. Authoritative DNS servers should be protected by Domain Name System (DNS) Security Extensions (DNSSEC).	FALSE	TRUE	FALSE	TRUE	TRUE	TRUE
29	Public Safety should establish and document a process to plan, test, evaluate and implement major change activities in an NG9-1-1 environment. To include NG9-1-1 implementations and other changes, new IP infrastructure, and NGCS.	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
30	NG9-1-1 Compliance Testing: Network Operators, Service Providers and Public Safety should establish and enforce policies that ensure Next Gen 9-1-1 services are in compliance with established Next Gen 9-1-1 standards and where possible should utilize an independent validation and verification process to validate Next Gen 9-1-1 standards compliance.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

NEW BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
31	Network Operators, Public Safety and Service Providers should ensure that policy-based routing controls for NG9-1-1 are implemented and managed to prevent adverse routing conditions.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
32	Prioritization in a NG9-1-1 SIP Environment: Network Operators, Service Providers and Public Safety should establish SIP Resource-Priority header value "esnet.1" to ensure that NG9-1-1 SIP packets are prioritized throughout the ESInet.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
33	Public Safety should provide Training to educate PSAP personnel as to the process to acquire/de-reference initial/updated/supplemental location information, as well as how to interpret location information received in an NG9-1-1 environment.	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
34	Network Operators, Public Safety (for NG9-1-1) and Service Providers should implement applicable industry standards to achieve interoperability between Real Time Text and TTY Baudot in support of emergency calling during the transition to end-state NG9-1-1.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
35	Network Operators, Service Providers and Public Safety should ensure that the NG9-1-1 system elements and the network elements between the OSP and the ESInet support the most accurate location information available to route 9-1-1 calls.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
36	Originating Service Providers (OSPs), Network Operators and Service Providers should design networks with redundant interconnectivity to Public Safety Emergency Services IP Networks (ESInets) using the characteristics of IP routing to maintain connectivity in the face of extensive disaster damage. OSPs may use diverse private facilities or their functional equivalent (e.g., MPLS, generic routing encapsulation (GRE) tunneling, virtual private network (VPN), or equally secure industry protocols) and where appropriate and supported by service level agreements.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE
37	Public Safety Emergency Services IP Networks (ESInets) should be designed, where technically and financially viable, with redundant interconnectivity to PSAPs using the characteristics of IP routing to maintain connectivity in the face of extensive disaster damage. Public Safety ESInets may use diverse private facilities or their functional equivalent (e.g., MPLS, generic routing encapsulation (GRE) tunneling, virtual private network (VPN), or equally secure industry protocols) and where appropriate and supported by service level agreements.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

NEW BP#	Best Practice Description	Property Manager	Equipment Supplier	Gov't	Network Operator	Service Provider	Public Safety
38	Originating Service Providers (OSPs) should route calls to the appropriate NG9-1-1 Next Generation Core Services (NGCS) based on the most accurate location information available. When location information is unavailable, OSPs should default route calls according to their internal policy, such as to an alternate call center.	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE
39	Network Operators and Service Providers should ensure that location information is made available to Public Safety as soon as is feasible after the 9-1-1 call commences.	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE
40	Network Providers, Service Providers and Public Safety (for NG9-1-1) should use secure network protocols such as TLS or IPsec for HTTP network interconnection for data acquisition of location and additional data provided by reference.	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE

2449

2450 # 18 Definitions

2451

Term	Description
ADR (Additional Data Repository)	A data storage facility for Additional Data. The ADR dereferences a request from the Next Generation Core Services (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. <from NENA MG [8]>
ANI (Automatic Number Identification)	Telephone number associated with the access line from which a call originates. <from NENA MG [8]>
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
BGCF (Breakout 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. <from NENA MG [8]>
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.

Term	Description
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. <from NENA MG [8]>
CSCF (Call Session Control Function)	General term for a functional entity within an IMS core network that can act as Proxy CSCF (P-CSCF), Serving CSCF (S-CSCF), Emergency CSCF (E-CSCF), or Interrogating CSCF (I-CSCF). <from NENA MG [8]>
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. <from NENA MG [8]>
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. <from NENA MG [8]>
GIS (Geographic Information System)	A system for capturing, storing, displaying, analyzing and managing data and associated attributes which are spatially referenced. <from NENA MG [8]>
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. <from NENA MG [8]>
HVAC (Heating, Ventilation, and Air Conditioning)	The system used to provide heating and cooling services to buildings. Attribution: Public Domain

Term	Description
IETF (Internet Engineering Task Force)	Lead standard setting authority for Internet protocols. <from NENA MG [8]>
ILEC (Incumbent Local Exchange Carrier)	A telephone company that had the initial telephone company franchise in an area. <from NENA MG [8]>
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. <from NENA MG [8]>
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. <from NENA MG [8]>
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. <from NENA MG [8]>
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. <from NENA MG [8]>
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. <from NENA MG [8]>

Term	Description
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. <from NENA MG [8]>
MF (Multi-Frequency)	A type of in-band signaling used on analog interoffice and 9-1-1 trunks. <from NENA MG [8]>
MGCF (Media Gateway Control Function)	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. <from NENA MG [8]>
MPC/GMLC (Mobile Position Center/Gateway Mobile Location Center)	The 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. <from NENA MG [8]>
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. <from NENA MG [8]>
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 <from NENA MG [8]>
NASNA (National Association of State 9-1-1Administrators)	An association that represents state 9-1-1 programs in the field of emergency communications. www.nasna9-1-1.org. <from NENA MG [8]>

Term	Description
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. <from NENA MG [8]>
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. <from NENA MG [8]>
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. <from NENA MG [8]> 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. <from NENA MG [8]> 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.

Term	Description
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. <from NENA MG [8]>
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. <from NENA MG [8]>
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. <from NENA MG [8]>
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. <from NENA MG [8]>
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 <from NENA MG [8]>
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, used by routing elements in the NG9-1-1 architecture to route an emergency call. See the NENA Master Glossary for more details. <from NENA MG [8]>

Term	Description
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. <from NENA MG [8]>
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. <from NENA MG [8]>
SRDB (Selective Routing Database)	The routing table that contains telephone number to ESN relationships which determines the routing of E9-1-1 calls. <from NENA MG [8]>
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). <from NENA MG [8]> 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. <from NENA MG [8]>

Term	Description
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. <from NENA MG [8]>
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 <from NENA MG [8]>
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. <from NENA MG [8]>
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). <from NENA MG [8]>
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.

19 References

[1] 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, 2017 https://www.atis.org/docstore/default.aspx
Non-Members use the ATIS Techstreet Store link and search for 0500034.

[2] ATIS-0700015, Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination, 2015 https://www.atis.org/docstore/default.aspx
Non-Members use the ATIS Techstreet Store link and search for 0700015.

[3] Task Force on Optimal Public Safety Answering Point Architecture (TFOPA – Main Page) https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point

[4] Task Force on Optimal PSAP Architecture **Final Report**, January 29, 2016 https://www.fcc.gov/document/fcc-releases-tfopa-final-report

[5] Task Force on Optimal PSAP Architecture **Supplemental Report**, December 2, 2016 https://transition.fcc.gov/pshs/9-1-1/TFOPA/TFOPA_WG1_Supplemental_Report-120216.pdf
[6] National Association of State 9-1-1 Administrators (NASNA) Model State 9-1-1 Plan https://www.911.gov/pdf/NASNA_and_National_911_Program_Model_State_911_Plan_2013.pdf
[7] NENA Standards & Best Practices are found at: http://www.nena.org/?page=Standards
[8] NENA Master Glossary: http://www.nena.org/?page=Glossary also available at: https://nenawiki.org/wiki/Category:Glossary
[9] NENA-INF-003.1-2013, NENA Potential Points of Demarcation in NG9-1-1 Networks Information Document, 2013 http://www.nena.org/?page=Standards
[10] The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 https://www.nist.gov/topics/cybersecurity
[11] Working Group 3: Network Reliability and Security Risk Reduction https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council
[12] FCC Best Practices website https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data
[13] FCC Public Safety and Homeland Security Bureau - Summary of 9-1-1 Certification Data for 2017 https://www.fcc.gov/document/summary-9-1-1-certification-data-2017
[14] Federal Communications Commission Report and Order and Further Notice of Proposed Rulemaking In the Matter of New Part 4 of the Commission's Rules Concerning Disruptions to Communications, FCC 04-188, ET Docket No. 04-35, August 19, 2004. https://www.fcc.gov/document/new-part-4-commissions-rules-concerning-disruptions-1
[15] Federal Communications Commission Report and Order, Further Notice of Proposed Rulemaking, and Order on Reconsideration, In the Matter of Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications, New Part 4 of the Commission's Rules Concerning Disruptions to Communications, and The Proposed Extension of Part 4 of the Commission's Rules Regarding Outage Reporting to Interconnected Voice Over Internet Protocol Service Providers and Broadband Internet Service Providers, FCC 16-63, PS Docket No. 15-80, ET Docket No. 04-35, and PS Docket No. 11-82, May 26, 2016. https://www.fcc.gov/document/part-4-ro-fnprm-and-order-reconsideration
[16] DHS - Cyber Risks to Next Generation 911 https://www.dhs.gov/sites/default/files/publications/NG911%20Cybersecurity%20Primer%20041816%20-%20508%20compliant_0.pdf
[17] FTC – Cybersecurity for Small Business https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
[18] NENA-STA-010 Detailed Functional and Interface Standards for the NENA i3 Solution http://www.nena.org/?page=Standards
[19] 3GPP TS 23.002 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network architecture. http://www.3gpp.org/specs/specs.htm