

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matters of)	
)	
911 Governance and Accountability)	PS Docket No. 14-193
)	
Improving 911 Reliability)	PS Docket No. 13-75

**POLICY STATEMENT
AND
NOTICE OF PROPOSED RULEMAKING**

Adopted: November 21, 2014

Released: November 21, 2014

By the Commission: Chairman Wheeler and Commissioners Clyburn and Rosenworcel issuing separate statements; Commissioners Pai and O’Rielly dissenting and issuing separate statements.

Comment Date: (45 days after date of publication in the Federal Register)

Reply Comment Date: (75 days after date of publication in the Federal Register)

TABLE OF CONTENTS

- I. INTRODUCTION 1
- II. BACKGROUND 5
 - A. Entities Providing 911 Connectivity 5
 - 1. Legacy TDM Architecture 8
 - 2. Transition to IP-Based and NG911 Networks 10
 - 3. Demarcation of Responsibility 15
 - B. Recent Outage Trends Reveal New 911 Network Reliability Challenges 19
 - C. Jurisdiction and Governance 28
 - D. Commission Framework for Reliable 911 Service 31
- III. POLICY STATEMENT 34
- IV. NOTICE OF PROPOSED RULEMAKING 36
 - A. Revisions to Rule 12.4 39
 - B. Ensuring Transparency and Accountability in Connection With Major Changes to Existing 911 Service 48
 - 1. Major Changes in 911 Service 49
 - 2. Discontinuance or Impairment of Existing 911 Services Essential to Call Completion 53
 - C. Ensuring Reliability and Accountability of New IP-Based 911 Capabilities and Services 57
 - D. Situational Awareness and Coordination Responsibility During 911 Outages 64
 - E. Legal Authority 76
- V. PROCEDURAL MATTERS 81
 - A. *Ex Parte* Presentations 81
 - B. Comment Filing Procedures 82
 - C. Accessible Formats 83
 - D. Regulatory Flexibility Act 84
 - E. Paperwork Reduction Act 85
 - F. Congressional Review Act 86

VI. ORDERING CLAUSES.....	87
APPENDIX A: PROPOSED RULES	
APPENDIX B: INITIAL REGULATORY FLEXIBILITY ANALYSIS	

I. INTRODUCTION

1. One of the fundamental purposes for which Congress created the Federal Communications Commission is to “promot[e] safety of life and property through the use of wire and radio communications.”¹ Nowhere does the Commission give higher expression to this overarching obligation than in its efforts to ensure that the American people have access to reliable and resilient 911 communications service. Since it was first introduced in 1968, 911 service has spread across the nation and become synonymous with emergency assistance.² These three digits – 911 – are now among the first phone numbers that parents teach to their children, and dialing 911 may be the most important call that we ever make. Accordingly, the American public has developed certain expectations with respect to the availability of 911 and E911 emergency services,³ and Commission action is both appropriate and necessary where reliance on voluntary efforts alone proves inadequate to ensure reliable and resilient 911 service.⁴

2. To be sure, this is not the Commission’s responsibility alone. State regulators and local emergency response agencies play critical roles in ensuring that 911 is available when needed and that every 911 call will be answered, and it is undoubtedly in the public interest that the Commission should work in close partnership with these stakeholders to carry out its responsibility. Nevertheless, we know that the technologies and commercial relationships that form the foundation of the 911 system are transitioning and, as a result, becoming increasingly interstate in nature. The Commission is uniquely positioned to ensure 911 reliability on a national scale and across different communications platforms and technologies, to promote the deployment of new and innovative 911 technologies by an increasingly diverse array of stakeholders, and to ensure that the benefits of advanced 911 service extend to all Americans.

3. The importance of ensuring nationwide 911 reliability as technologies transition has been underscored by several recent disruptions of 911 service that have affected the public in multiple states or across the entire nation. While innovative technologies have the potential to improve many aspects of 911 service and enhance the ability of first responders to do their jobs more effectively, these recent outages have revealed that technology changes may also introduce new vulnerabilities. As the Commission concluded in extending 911 obligations to interconnected VoIP providers in 2005, “. . . new communications technologies have posed technical and operational challenges to the 911 system, necessitating the adoption of a uniform national approach to ensure that the quality and reliability of 911 service is not damaged by the introduction of such communications technologies.”⁵ While we have

¹ 47 U.S.C. § 151.

² See Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys., CC Docket No. 94-102, *Report and Order and Further Notice of Proposed Rulemaking*, 11 FCC Rcd. 18676, 18678 ¶ 3 (1996) (observing that “[d]ialing 911 is the most effective and familiar way the American public has of finding help in an emergency”).

³ See IP-Enabled Services; E911 Requirements for IP-Enabled Service Providers, WC Docket Nos. 05-196, 04-36, *First Report and Order and Notice of Proposed Rulemaking*, 20 FCC Rcd. 10245, 10249 ¶ 6 (2005) (*VoIP 911 Order*).

⁴ See Reliability and Continuity of Communications Networks, Including Broadband Technologies, PS Docket Nos. 13-75, 11-60, *Report and Order*, 28 FCC Rcd 17476, 17487, ¶ 30 (2013) (*911 Reliability Order*) (concluding that “we are not persuaded that additional voluntary measures alone would provide adequate assurance of a reliable and resilient 911 system”).

⁵ *VoIP 911 Order*, 20 FCC Rcd at 10263, ¶ 30.

previously undertaken to monitor the transition to Next Generation 911 (NG911) technologies to determine whether our rules should be revised or expanded to cover new best practices or additional entities,⁶ recent events have demonstrated that the pace of change already requires prompt action to review these vulnerabilities. Failure to take appropriate action risks undermining the reliability and resiliency of current 911 services and endangering the transition to NG911 technologies that offer even greater public safety benefits. The American public must have confidence that 911 will work every time help is needed. Any failure to meet this expectation puts individual lives at stake and erodes vital public trust in our nation's emergency services. We must address these critical issues now, before even larger 911 outages put more Americans at risk.

4. In this *Policy Statement and Notice of Proposed Rulemaking*, we affirm the core principles that have guided and will continue to guide the Commission's approach to ensuring reliable and resilient 911 service and its continuing partnership with state and local authorities. We propose specific rules designed to address failures leading to recent multi-state 911 outages, based on the October 2014 report of the Public Safety and Homeland Security Bureau.⁷ Finally, we propose additional mechanisms designed to ensure that our 911 governance structure keeps pace with evolving technologies and new reliability challenges so that all 911 service providers remain fully accountable to the public they serve.

II. BACKGROUND

A. Entities Providing 911 Connectivity

5. The architecture of 911 networks, both legacy and NG911, can include multiple entities, which each provide one or more links in a chain of connectivity that begins with a caller seeking emergency assistance and ends at a 911 call center known as a public safety answering point (PSAP). The 911 ecosystem includes entities necessary for completion of voice calls and other communications to 911⁸, as well as those that provide automatic location information (ALI), automatic number information (ANI), location information services (LIS), text-to-911 capabilities, and the transmission of multimedia information in an NG911 environment. These entities include several distinct types of communications providers, including originating service providers (OSPs), incumbent local exchange carriers (ILECs), system service providers (SSPs),⁹ subcontractors and vendors that provide additional technical capabilities, and PSAPs and emergency authorities themselves to the extent that they provide 911 network components.

6. Each part of the 911 ecosystem plays a unique role in reliable call completion, and those roles are changing as technologies evolve. Generally, however, 911 communications originate on the OSP network where the caller is located, which may be a landline telephone network, a wireless network, or an over-the-top (OTT) communications service operating over another network. Calls, text messages

⁶ *Id.* at 17533, ¶ 159 (undertaking review of rules in five years).

⁷ FCC Public Safety & Homeland Security Bureau, *April 2014 Multistate 911 Outage: Cause and Impact*, PS Docket No. 14-72, PSHSB Case File Nos. 14-CCR-0001-0007 (Oct. 2014), available at <http://www.fcc.gov/document/april-2014-multistate-911-outage-report> (*Multistate 911 Outage Report*).

⁸ This includes functions used to connect legacy and NG911 components, such as legacy network gateways (LNGs).

⁹ A system service provider (SSP) provides systems and support necessary to enable 911 calling for one or more PSAPs in a specific geographic area. It is typically, but not always, an ILEC. SSP functionalities may include interconnection with other telecommunications providers, routing of 911 calls, delivery of location and number information, and coordinating with PSAP authorities and other telecommunications entities for troubleshooting and disaster mitigation and recovery. SSPs may also install PSAP call handling equipment and train PSAP personnel when contracted to do so. See Enhanced 9-1-1 System Service Provider (E9-1-1SSP), NENA Master Glossary of 9-1-1 Terminology, NENA ADM-000.17, September 9, 2013, available at www.nena.org/resource/collection/625eab1d-49b3-4694-b037-8e854b43ca16/NENA-ADM-000.17_Master_Glossary_20130909.pdf.

and other data then enter a 911 network that is shared by many or all OSPs, which provides a routing capability that may be physically based on switched circuits or logically based on software and databases. The 911 network delivers calls and data to the appropriate PSAP, where trained call-takers determine the nature of the emergency and dispatch first responders.

7. Our goal of proactive, measured accountability for reliable 911 call completion extends from the provision of service to the 911 caller at one end to the provision of service to the PSAP on the other. In technical terms, it includes the communications networks required to initiate 911 calls and deliver those calls, with associated number and location information, including the networks necessary for OTT services to connect consumers to PSAPs when they dial 911 or send text messages or other data.¹⁰ Jurisdictionally speaking, the concept includes the shared authority of the federal government and states to collectively oversee all components of 911 service. These roles are not mutually exclusive and leave room for states and localities to take action within their jurisdictions based on the unique circumstances and needs of their constituents. We also rely on state and local oversight to ensure that our combined governance covers every link in the chain of 911 service nationwide.

1. Legacy TDM Architecture

8. The most basic function of a 911 network is to route emergency calls to the appropriate PSAP based on the caller's location. Historically, legacy 911 networks have relied on circuit-switched time division multiplexing (TDM) architecture to provide this capability. At a basic level, this architecture can be divided into three segments: (1) origination, (2) routing, and (3) delivery of calls to a PSAP. In the call origination segment, a caller dials 911 through a home telephone, wireless phone, or interconnected VoIP device. The OSP transmits the 911 call, with location and other information applicable to its service,¹¹ to a selective router¹² operated by a 911 service provider.¹³ In the routing segment, the 911 service provider directs the call via the selective router to the appropriate PSAP based on the caller's location. Finally, the call is delivered to the PSAP, where it is answered by a 911 operator

¹⁰ The scope of this proceeding would not, however, include factors such as the design and manufacture of communications devices or operating systems where they are not part of a 911 service relationship between consumers and PSAPs.

¹¹ Calls to 911 from a wireline home telephone travel through the local switch serving that subscriber, then to the selective router. Because the mobility of wireless subscribers makes permanent street addresses unsuitable as location indicators, routing wireless 911 calls and locating wireless callers requires use of real-time location information. Wireless 911 calls use the sector of the originating cell tower to provide an approximate location and travel through a switch called a mobile switching center (MSC) before reaching the selective router. Similarly, because interconnected VoIP users may place 911 calls from outside their home areas, a permanent telephone number cannot be used for routing. The Commission requires interconnected VoIP providers to obtain a "registered location" from subscribers when they first initiate service and when they change their physical location. *See* 47 C.F.R. § 9.5(d)(1)-(2).

¹² Selective routing is the ability of a network to select the appropriate destination PSAP for a 911 call based on the location associated with the caller's ANI. It allows the 911 network to deliver calls to a PSAP based on service areas of the public safety agency instead of being based on the exchange or rate center coverage of a particular telecommunications carrier's switching equipment. *See* NENA Standard 03-005, Generic Requirements for an Enhanced 9-1-1 Selective Routing Switch at 12, § 2.21 (January 2004), *available at* http://c.ymcdn.com/sites/www.nena.org/resource/collection/1F053CE7-3DCD-4DD4-9939-58F86BA03EF7/NENA_03-005-v1_Generic_Requirements_E9-1-1_SR_Switch.pdf.

¹³ As noted above, 911 capabilities or network components may be provided by a broad range of entities. Here, we refer to the "911 service provider" as the entity that provides 911 service to a PSAP under a direct contractual relationship with that PSAP or emergency authority, as opposed to a sub-contractor relationship with other service providers. This entity is often, but not always, the ILEC in that jurisdiction. *See also* 47 C.F.R. § 12.4(a)(4) (defining "covered 911 service provider" for purposes of our rules).

using customer premises equipment (CPE)¹⁴ to assist in dispatching first responders. The PSAP queries an ALI database to obtain more precise information on the location of the caller.¹⁵ Thus, in addition to supporting the transmission of 911 calls themselves, 911 networks must also support the transmission of call-back and location information associated with each call.

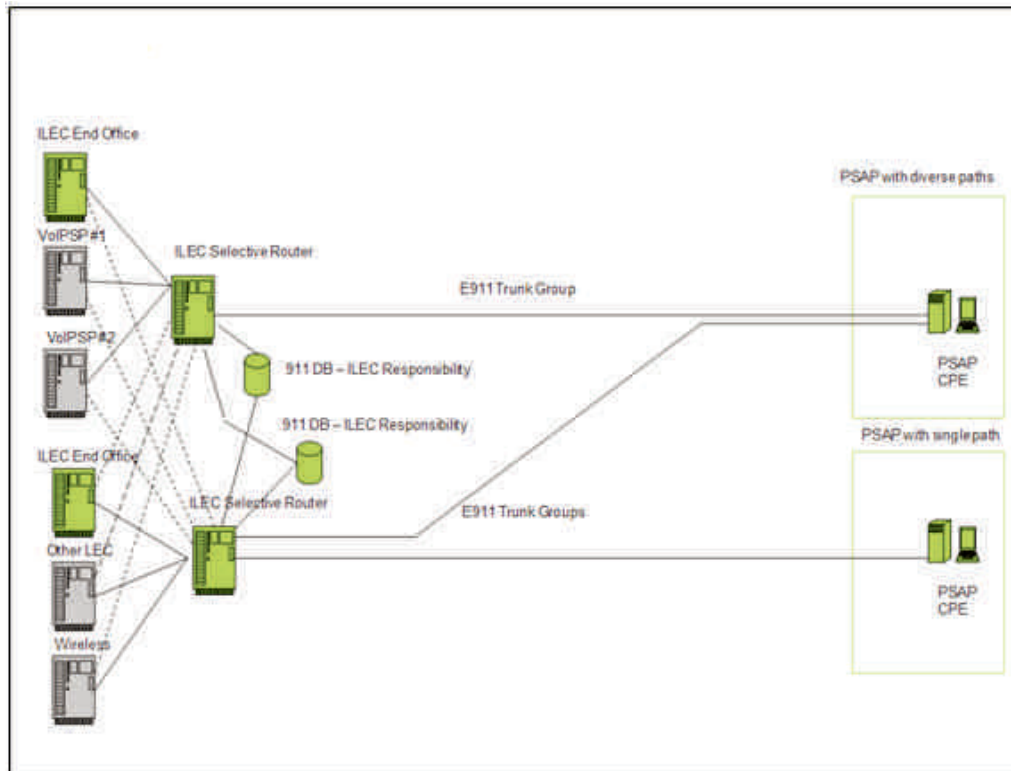


Figure 1: Enhanced 911 (E911) Network Architecture¹⁶

9. This basic architecture has evolved over the years as specialized SSPs increasingly have begun to complement or replace incumbent carriers' existing capabilities in each segment of 911 service. For example, wireless carriers commonly contract with SSPs to provide the location information required with each originating call. Vendors may also provide 911 call routing capabilities to ILECs or sell CPE to PSAPs as part of their 911 service.¹⁷ Some SSPs have been performing these functions for more than

¹⁴ See NENA Master Glossary of 9-1-1 Terminology, NENA-ADM-000.18-2014 at 58 (July 29, 2014), available at http://c.y.mcdn.com/sites/www.nena.org/resource/resmgr/Standards/NENA-ADM-000.18-2014_2014072.pdf (defining CPE as “[c]ommunications or terminal equipment located in the customer’s facilities” or “[t]erminal equipment at a PSAP”).

¹⁵ For wireline calls, ALI is based on the address associated with the caller’s phone number. For wireless calls, providers use various technologies to determine the caller’s location.

¹⁶ See *Multistate 911 Outage Report* at 14. This diagram is representative of legacy E911 network architecture generally but is not intended to cover every possible deployment of E911 technologies. Network configurations among different E911 service providers and service areas may vary.

¹⁷ Under the governance framework described below, decisions regarding purchasing, maintenance, and operation of CPE have primarily been left to state and local authorities. Some covered 911 service providers, however, also sell, re-sell, or support and maintain CPE. In keeping with this framework, the proposals in this *NPRM* focus on

(continued....)

20 years, while others are relatively new entrants. More recently, PSAPs and state or local emergency authorities that contract for 911 services may specify advanced capabilities that have not historically been provided by carriers and can only be supplied by specialized SSPs. These developments are not new – in fact, SSPs and technical vendors have played major roles in the development of Enhanced 911 (E911) service – but they have generally occurred within the overall network architecture described above, based on relationships between 911-related entities in a legacy environment, as described below.

2. Transition to IP-Based and NG911 Networks

10. Like communications networks generally, 911 networks are evolving from TDM-based architectures to Internet Protocol (IP)-based architectures. Ultimately, the TDM-based legacy 911 infrastructure will be replaced by NG911 networks that rely entirely on IP-based technologies. NG911 has the potential to vastly improve 911 service by offering more flexible call routing and providing PSAPs with a greater range of information, including text, video, and other data from devices such as vehicle crash sensors. If designed to mitigate known risks of failure and deployed with proper operational safeguards, NG911 networks can also be more reliable than their TDM-based counterparts.

11. A key component of NG911 architecture is the emergency services IP network (ESInet), which is an IP-based “network of networks” that can be shared by all public safety agencies that may be involved in any emergency.¹⁸ An ESInet is typically deployed at the state or regional level and operated under contract with those PSAPs that share its capabilities or through a state or regional government agency. In the NG911 environment, OSPs contract with entities that determine the appropriate ESInet to receive each call, and may also physically route calls to the specified ESInet. The OSP may also connect directly to an ESInet and use an IP-based emergency call routing function to determine where to deliver 911 calls and associated data. Location databases, typically operated by an ILEC or SSP, then allow PSAPs and other authorized entities to query for the geographic location of a specific caller. These functions may be provided by one covered 911 service provider or several depending on how NG911 is deployed in a particular area.

(Continued from previous page) _____
accountability of covered 911 service providers, who may also be CPE vendors, not on purchasing decisions by PSAPs.

¹⁸ See Detailed Functional and Interface Standards for the NENA i3 Solution, 08-003 v1, (June 14, 2011), available at https://www.nena.org/?page=i3_Stage3

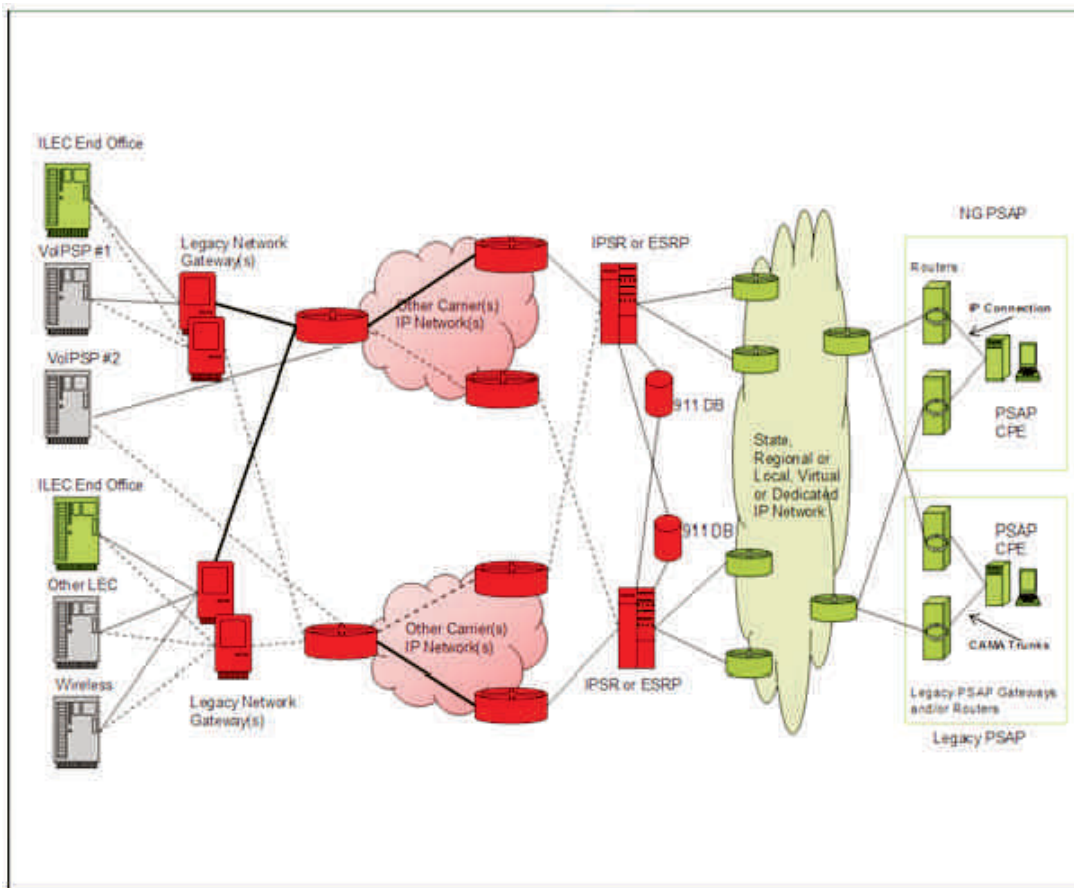


Figure 2: NG911 Network Architecture¹⁹

12. The transition to IP-based 911 networks is part of a broader set of “historic technology transitions that are transforming our nation’s voice communications services.”²⁰ The Commission, in the January 2014 *Technology Transitions Order*, identified “public safety and national security . . . including the ability of the public to reach 911” as one of the “enduring values” that must be preserved throughout these technology transitions.²¹ To that end, the Commission has required applicants for “service based experiments” to “[p]reserve 911/E911 and Next Generation 911 capabilities” and stated that “we expect PSAPs to be provided with at least the same level of network access, resiliency, redundancy, and security that they enjoy under agreements and tariffs currently framing the legacy emergency network.”²²

13. The retirement of legacy infrastructure and the transition period in which multiple technologies may be in use simultaneously, however, raise reliability and interoperability challenges that

¹⁹ See *Multistate 911 Outage Report* at 15. During the transition to NG911, IP-based networks may extend all the way to NG911-enabled PSAPs, or to a gateway that routes calls to legacy PSAPs via centralized automatic messaging accounting (CAMA) trunks. Both examples are shown above.

²⁰ See *Technology Transitions*, GN Docket No. 13-5, *Order, Report and Order, and Further Notice of Proposed Rulemaking*, 29 FCC Rcd. 1433, ¶ 1 (2014) (*Technology Transitions Order*).

²¹ *Id.* at ¶ 38.

²² *Id.*

cannot be ignored. IP-based 911 networks are more geographically diverse than their legacy counterparts and are likely to provide more services such as 911 call routing and ALI across multiple states and jurisdictions. In comparison to legacy 911 networks, IP-based networks rely more on remote servers and databases rather than locally situated switch-based components to support key 911 functions. Even as they make new capabilities possible, these changes in network architecture also raise new issues and vulnerabilities that did not exist in the legacy 911 environment. In many instances, IP-based network components are being introduced into 911 networks on a piecemeal basis rather than through full implementation of NG911. Thus, in many jurisdictions, 911 service is provided through transitional architecture that includes both IP-based and TDM-based components.

14. The transition to IP-based architecture is also altering the identity, relationships, and roles of 911 service providers. While most legacy 911 services were provided by incumbent carriers, evolving technologies have allowed a growing number of entities – both carriers and non-carrier SSPs – to offer 911 capabilities, or more specialized components within the chain of connectivity previously provided by a single entity. For example, a PSAP may contract with an ILEC for 911 services, but the ILEC may then sub-contract with a third-party vendor to route those calls and provide ALI from databases that may be populated by multiple providers and may be located in a different state. In other cases, a PSAP may contract directly with a non-carrier SSP for call routing and ALI capabilities, bypassing the traditional role of the carrier entirely.

3. Demarcation of Responsibility

15. The demarcation of responsibility for each segment of a 911 call traditionally has been straightforward. OSPs are responsible for transmitting their customers' 911 calls to a selective router, which is typically operated by the ILEC in each jurisdiction.²³ The ILEC operating the selective router is responsible for routing those calls to the appropriate PSAP. State and local authorities operating the PSAP are then responsible for answering the call and dispatching help.

16. A similar demarcation of responsibility has applied to troubleshooting and recovery from 911 outages within the traditional architecture. Historically, ILECs have operated most or all of the network infrastructure required to route and deliver 911 calls to PSAPs and have contracted with PSAPs and emergency authorities to provide those capabilities. Many ILECs, or their affiliates, have also sold, installed, and maintained PSAP CPE, although this market has grown increasingly competitive. Accordingly, ILECs typically have had both a contractual relationship with the PSAPs they serve and primary responsibility for technical support and information sharing under tariffs and other state regulations governing the scope of 911 services offered to PSAPs.²⁴ Under this arrangement, a PSAP's primary contact in the event of an outage would be its 911 service provider – typically the ILEC or an affiliate of the ILEC that distributes and maintains CPE – which would have the ability to maintain situational awareness across the 911 network and coordinate with other providers to mitigate and resolve disruptions in service. While such relationships have grown increasingly complex over the years as new entities compete to provide 911 capabilities, PSAPs continue to expect rapid and responsive support if any portion of the 911 network fails, irrespective of the type or number of entities providing services within the 911 call chain.

²³ See Revision of the Commission's Rules To Ensure Compatibility with Enhanced 911 Emergency Calling Systems; Request of King County, Washington, CC Docket No. 94-102, *Order on Reconsideration*, 17 FCC Rcd 14789, ¶ 1 (2002) (*King County Decision*).

²⁴ Certain communications providers already have specific responsibilities under Part 4 of the Commission's rules to notify PSAPs of disruptions in 911 service. See 47 C.F.R. § 4.9(a), (c), (e)-(g) (requiring cable, satellite, wireline, wireless, and interconnected VoIP providers to notify affected PSAPs of any outage that "potentially affects a 911 special facility," as defined in 47 C.F.R. § 4.5(e). "Covered 911 service providers" – those that provide core 911 capabilities directly to PSAPs – must notify PSAPs within 30 minutes of discovering an outage and follow up with more detailed information within two hours. The information-sharing proposals in this *NPRM* are intended to complement and strengthen, not to replace or modify, existing responsibilities under Part 4.

17. Without appropriate safeguards, both the evolution of 911 service and the ultimate goal of an all-IP 911 infrastructure have increased the number of potential failure points in the delivery of 911 service.²⁵ In early wireline 911 networks, a single company may have controlled the provision of all 911 network services for each jurisdiction. Support for 911 calls from wireless phones and interconnected VoIP devices requires interconnection among carriers and has increasingly created a role for SSPs and vendors to provide more specialized capabilities. Some incumbent carriers may also be planning to reduce their support for end-to-end 911 service, instead offering wholesale network transport capabilities to more specialized SSPs. Where incumbents seek to exit the market for 911 services or shift to playing different roles with new entrants taking their place, and as 911 networks continue to evolve, 911 governance mechanisms must adapt to ensure that new network architectures and relationships between PSAPs, service providers, and regulators remain transparent and dependable. If a problem occurs, it is vital that PSAPs experiencing a 911 outage receive timely notification and information regarding the scope of the outage and options for mitigation.²⁶ The contracting out of certain aspects of one service provider's functions, or the determination of a PSAP to contract with more than one entity for various aspects of 911 service, does not absolve individual entities of their respective obligations for 911 service.²⁷

18. Well-established legal principles “ordinarily make principals or employers vicariously liable for the acts of their agents or employees in the scope of their authority or employment.”²⁸ Section 217 of the Communications Act specifically codifies this principle with respect to “any officer, agent, or other person acting for or employed by any common carrier.”²⁹ Quite apart from Section 217, however, “[t]he Commission has long held that licensees and other regulatees are responsible for the acts and omissions of their employees and independent contractors,” and has recognized that “under long established principles of common law, statutory duties are nondelegable.”³⁰ However, beyond questions of legal liability – which often take significantly longer to resolve – PSAPs and service providers alike must have accurate information and clear expectations of whom to contact if something goes wrong, when every second matters and unnecessary delays put public safety at risk. Effective 911 governance must work in real time, while protecting and enforcing legal rights and obligations in the long term. We therefore believe that changing relationships between covered 911 service providers and the complexities of multi-state NG911 architecture call for more specific governance mechanisms to ensure proactive, measured accountability and situational awareness throughout the present and future 911 ecosystem.

²⁵ We do not address here the application of the *King County Decision* to ESInets and other NG911 network components and defer for another day the complex issues of interconnection and cost recovery in an NG911 environment. Our discussion here is limited to the effect of changing network architectures on 911 governance and mechanisms to promote reliability and accountability across the nation's 911 networks.

²⁶ See 47 C.F.R. § 4.9.

²⁷ See 47 C.F.R. § 64.3001 (“All telecommunications carriers shall transmit all 911 calls to a PSAP, to a designated statewide default answering point, or to an appropriate local emergency authority.”); 47 C.F.R. § 20.18(b) (“CMRS providers subject to this section must transmit all wireless 911 calls without respect to their call validation process to a Public Safety Answering Point.”); 47 C.F.R. § 9.5(b)(2) (“Interconnected VoIP service providers must transmit all 911 calls, as well as ANI and the caller's Registered Location for each call, to the PSAP, designated statewide default answering point, or appropriate local emergency authority that serves the caller's Registered Location.”).

²⁸ *Meyer v. Holley*, 537 U.S. 280, 285 (2003).

²⁹ 47 U.S.C. § 217.

³⁰ *Eure Family Limited Partnership, Memorandum Opinion and Order*, 17 FCC Rcd 21861, 21863-64 (2002), citing *MTD, Inc.*, 6 FCC Rcd 34, 35 (1991), *Wagenvoord Broadcasting Co.*, 35 F.C.C.2d 361 (1972). See also *Amendment of the Commission's Rules to Provide Spectrum for the Operation of Medical Body Area Networks, First Report and Order and Further Notice of Proposed Rulemaking*, 17 FCC Rcd 6422, 6439 n.108 (2012); *Courier Communications Corp.*, 23 FCC Rcd 2593, 2595 n.25 (EB 2008).

B. Recent Outage Trends Reveal New 911 Network Reliability Challenges

19. The Commission's past efforts to promote reliable and resilient 911 service have focused on minimizing risks to legacy 911 infrastructure, particularly during natural disasters and other large-scale emergencies. The June 2012 derecho storm, for example, disrupted 911 service in six states, due in large part to insufficient physical diversity of critical 911 circuits and faulty or inadequate backup power in the central offices of ILECs. After investigating these outages, the Commission responded by adopting rules requiring certain 911 service providers to take reasonable measures to provide reliable service with respect to circuit diversity, backup power, and network monitoring capabilities.³¹ These rules apply to "covered 911 service providers," defined generally as those that provide core 911 capabilities "directly to a PSAP."³² Thus, providers subject to reliability certification rules will typically be those that operate the portion of the 911 network between the selective router and the central office serving each PSAP, not those that originate 911 calls or provide NG911 capabilities that are not the "functional equivalent" of legacy 911 service.³³ Other Commission rules, however, require certain OSPs to "transmit all 911 calls to a PSAP"³⁴ and notify PSAPs of disruptions in 911 service.³⁵ Together, these rules reflect the principle that all service providers in the chain of 911 service – from origination to completion – must be accountable for reliable service and responsive in the event of an outage.

20. While legacy 911 infrastructure remains in use throughout much of the country, recent events have shown that evolving technology, while providing many benefits to PSAPs and the public, also has introduced new and different risks. A growing number of disruptions to 911 service are caused by software malfunctions, database failures, and errors in conversion from legacy to IP-based network protocols. These failures may occur in portions of the network that are not directly analogous to the legacy architecture based on selective routers and central offices. Moreover, these new modes of failure have the potential to affect many states at once, or even all of a service provider's customers nationwide. While IP-based networks offer the potential for increased redundancy and resiliency, the consolidation of critical resources in a small number of databases increases the risk of a catastrophic failure affecting numerous customers.

21. For example, in April 2014, a software coding error at a Colorado-based SSP's 911 call routing facility led to a loss of 911 service to a population of more than 11 million in seven states – California, Florida, Minnesota, North Carolina, Pennsylvania, South Carolina, and Washington – for up to six hours.³⁶ More than 6,600 calls to 911 never reached a PSAP.³⁷ The call routing software was designed to keep track of the trunk assignment for 911 calls assigned to numerous PSAPs around the nation that relied on centralized automatic messaging accounting (CAMA) trunking, a legacy TDM type of 911 trunk.³⁸ The coding error caused the software to stop making trunk assignments, preventing calls routed through the Colorado hub from reaching 81 PSAPs in seven states.³⁹ Inadequate alarm management resulted in significant delays in identifying the software fault and restoring 911 service to

³¹ See 47 C.F.R. § 12.4; *911 Reliability Order*, 28 FCC Rcd at 17492-93, ¶¶ 45-48.

³² 47 C.F.R. § 12.4(a)(4); *911 Reliability Order*, 28 FCC Rcd at 17488-89, ¶ 36.

³³ See 47 C.F.R. § 12.4(a)(4)(i)(A).

³⁴ See 47 C.F.R. §§ 64.3001 (telecommunications carriers); 20.18(b) (CMRS providers); 9.5(b)(2) (Interconnected VoIP providers).

³⁵ See 47 C.F.R. § 4.9.

³⁶ *Multistate 911 Outage Report* at 1.

³⁷ *Id.*

³⁸ *Id.* at 3.

³⁹ *Id.*

full functionality.⁴⁰ The SSP operated a redundant hub in Florida to which 911 traffic could have been immediately rerouted, but because the malfunction was not detected promptly, it did not execute either an automatic or manual switchover of traffic until six hours had elapsed.⁴¹ Furthermore, affected PSAPs reported confusion and frustration regarding communications with their 911 service providers during the outage, citing a lack of information about the cause of the outage and whether the SSP or incumbent carrier was responsible for repairs.⁴²

22. An inquiry by the Public Safety and Homeland Security Bureau found that the widespread impacts of this outage in multiple states provided “a vivid example of the vulnerabilities that IP-supported architectures may present, without sufficient network safeguards and clear lines of accountability.”⁴³ The Bureau also noted that “[w]hat is most troubling is that this is not an isolated incident or an act of nature,” but one of an increasing number of “sunny day” 911 outages caused by preventable errors in software and database configuration and maintenance.⁴⁴ Notably, these outages have disrupted access to 911 even while communications networks in general have remained functional.⁴⁵ The Bureau recommended a range of Commission actions in response to this trend,⁴⁶ adding that “[t]he introduction of NG911 and IP-based technologies will require industry as well as state, local, tribal and territorial governments and commissions to move aggressively to ensure that technology enabled optimization does not introduce unacceptable risks that threaten imperiling 911 reliability and resiliency.”⁴⁷ The Bureau coordinated its inquiry into the outage with a parallel investigation by the Washington Utilities and Transportation Commission, providing an example of such cooperation between federal and state authorities.⁴⁸

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² See Comments of the Washington State E911 Coordinator’s Office at 2-3 (“Neither Century Link nor Intrado provided any instructions to PSAPs on what they could do to mitigate the outage. The PSAPs were left on their own to try to figure out how to provide some level of service to the public. Because of the confusion and lack of instruction, as to the nature of this outage, a work-around that worked successfully for one PSAP, such as going to their back-up, did not work for other PSAPs.”). There is, however, a factual dispute regarding the extent of communications between service providers and affected PSAPs. See Comments of CenturyLink, PS Docket No. 14-72 at 7 (June 16, 2014) (stating that CenturyLink “began notifying the affected PSAPs by telephone, but at that time the full scope of the outage was not yet known” and that “CenturyLink continued reaching out to additional affected PSAPs and the Washington State E911 Coordinator’s Office and making test calls as the wide scope of the outage became clearer through the early morning hours of April 10, 2014, and was ultimately resolved”).

⁴³ *Multistate 911 Outage Report* at 1, 26.

⁴⁴ *Id.* at 1.

⁴⁵ *Id.* at 7, 8, 20 (noting that customers who called 911 during the April multistate outage had a dial tone but received a busy signal).

⁴⁶ See *id.* at 25-26 (recommending that the Commission develop and implement NG911 transition best practices; conduct further proceedings on 911 reliability; promote improved situational awareness and information sharing among governmental and commercial stakeholders; and “use enforcement action as necessary to safeguard reliable end-to-end 911 service”).

⁴⁷ *Id.* at 2.

⁴⁸ David W. Danner, Chairman of the Washington Utilities and Transportation Commission, attended the Commission meeting where the *Multistate 911 Outage Report* was presented and underscored the importance of “an ongoing dialog and collaboration between the FCC and states.” He added that “[i]t makes sense for us to share information where we can to identify problems that are common among the states and develop strategies to address them.” See October 2014 Open Commission Meeting, Video at 93:10-93:50, *available at* <http://www.fcc.gov/events/open-commission-meeting-october-2014>.

23. In addition, the state of Hawaii has experienced multiple disruptions in 911 service since January 2014, following the installation of an NG911 network serving PSAPs on each island.⁴⁹ In the largest of these outages, calls to 911 received a busy signal intermittently or completely for one hour and 32 minutes, and PSAPs lost access to ANI and ALI for nearly seven hours.⁵⁰ Sixty-nine unique wireline calls and an unknown number of wireless calls to 911 could not be completed.⁵¹ Other outages resulted in the intermittent or complete failure of 911 calls for five, 20, 41, and 50 minutes respectively, as well as disruptions in ANI and ALI as long as five hours.⁵² A report to the Hawaii Enhanced 9-1-1 Board found two common themes in these outages: (1) many of the incidents occurred during planned maintenance activities or during an installation or upgrade of the NG911 system, and (2) the incidents typically involved limitations in the ability of NG911 network routers to accommodate higher-than-anticipated levels of network traffic.⁵³

24. In August 2014, a similar NG911 outage disrupted 911 service to the entire state of Vermont. The outage lasted 40 minutes and blocked 83 calls to 911, according to news reports.⁵⁴ The affected service provider described the cause as a “double equipment failure” and another error during system restoration that caused the network to be temporarily unavailable.⁵⁵ Although the Vermont Enhanced 911 Board noted that “it appears that everyone who had an emergency was able to get help through their local police or other emergency responders,” the Board stated that it was “disappointed with the performance of our technology vendor, both for the fact that the system failed and also for the time it took to get the call back numbers for those who were not able to get through to 911 during the outage.”⁵⁶

25. Also in August 2014, more than 40 million people nationwide lost access to 911 for more than two hours due to a major wireless carrier 911 outage, underscoring the importance of OSP networks in reliable 911 call completion.

26. Unlike the 2012 derecho outages and many other more localized disruptions to 911 service in the legacy environment, the incidents described above did not result from a natural disaster, a loss of commercial power, or an unusually high call load associated with an emergency. Rather, these systems failed under everyday conditions due to an unexpected malfunction or a seemingly-routine software update that produced unintended consequences. Although the affected networks were designed to be redundant, these outages also show how easily that redundancy can be compromised if critical components fail, and how serious and far-reaching the effects can be when 911 infrastructure is consolidated across multiple regions or states.

27. Furthermore, the scope and severity of the outages was not immediately apparent because of incomplete situational awareness, complicated by the logistical difficulties of coordinating recovery across multiple service providers and vendors. As a result, there was a significant period of time when 911 calls were simply being dropped rather than being rerouted to alternate PSAPs or backup servers. Although the affected providers report making changes in the networks and processes to prevent these

⁴⁹ See Letter from Ben Morgan, Vice President of Customer Care and Network Reliability, Hawaii Telcom, to Hawaii Enhanced 9-1-1 Board (Sept. 5, 2014).

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² *Id.*

⁵³ *Id.*

⁵⁴ See Brent Curtis, *Vermont Probes Blackout of 911*, THE BARRE MONTPELIER TIMES ARGUS, Aug. 8, 2014, available at <http://www.timesargus.com/article/20140808/NEWS03/708089908> (last accessed Aug. 28, 2014).

⁵⁵ See Press Release, E9-1-1 Outage Being Investigated, Vermont Enhanced 9-1-1 Board, Aug. 7, 2014, available at <http://vtdigger.org/2014/08/07/e-911-outage-investigated/> (last accessed Aug. 28, 2014).

⁵⁶ *Id.*

failures from recurring, we remain concerned that the outages discussed above reflect broader issues that extend beyond any single entity and must be addressed holistically.

C. Jurisdiction and Governance

28. Governance of legacy 911 is shared between the state, local, and federal levels, allowing for a range of localized approaches to achieving nationwide objectives of ubiquitous and reliable 911 service. The local structure and provision of 911 service by PSAPs is typically a state law matter, with some states further delegating aspects of 911 governance to the local level.⁵⁷ In addition, many states regulate the provision of 911 service by incumbent carriers under tariff regulations issued by the state public utility or public service commission.⁵⁸ As the Commission observed in 2005, “[r]esponsibility for establishing and designating PSAPs or appropriate default answering points, purchasing customer premises equipment, retaining and training PSAP personnel, purchasing 911 network services, and implementing a cost recovery mechanism to fund all of the foregoing, among other things, falls squarely on the shoulders of states and localities.”⁵⁹ Accordingly, citing “significant questions of federalism” and “a strong consensus among commenters that the Commission should not interfere with the internal operations of PSAPs”⁶⁰ the Commission has declined to impose reliability certification requirements on governmental authorities that provide their own 911 capabilities.⁶¹ In the *911 Reliability Order*, the Commission added that “[t]o the extent that commenters express concern about the appropriate line between federal and state authority with respect to 911 service, we emphasize that the Commission’s actions here will be undertaken, consistent with past practice, in partnership with such authorities and in light of their unique interest in the delivery of reliable 911 service.”⁶² We propose to take the same approach here as in the *911 Reliability Order*: the proposals in this *NPRM* are not intended to alter state jurisdiction over 911 or to limit state and local authorities’ ability to take consistent action.⁶³ Indeed, Congress has clearly recognized the important role that States and localities can play in ensuring reliable 911 service, both by directing the Commission to “encourage and support efforts by States” in this area⁶⁴ and by directing NTIA and NHTSA to establish a joint program to facilitate coordination and communication with state and local emergency personnel, backed by federal grants.⁶⁵ The Commission will work with NTIA, NHTSA, and other federal partners to strongly support States in their exercise of that authority.

29. Congress has, however, directed the Commission to “designate 911 as the universal emergency telephone number within the United States for reporting an emergency to appropriate

⁵⁷ See Federal Communications Commission, Legal and Regulatory Framework for Next Generation 911 Services, Report to Congress and Recommendations § 3.2.1 (2013), available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-319165A1.pdf (*NG911 Report*).

⁵⁸ *Id.*

⁵⁹ *VoIP 911 Order*, 20 FCC Rcd. at 10249, ¶ 7.

⁶⁰ *911 Reliability Order*, 28 FCC Rcd at 17490-91, ¶ 41.

⁶¹ See *id.*; 47 C.F.R. § 12.4(a)(4)(ii)(A).

⁶² *911 Reliability Order*, 28 FCC Rcd at 17530-31, ¶ 150.

⁶³ See *id.* (FCC adoption of 911 reliability rules “is not intended to preempt state and local actions so long as they do not operate to frustrate the implementation of the Commission rules”).

⁶⁴ 47 U.S.C. § 615 (directing the Commission to “encourage and support efforts by States to deploy comprehensive end-to-end emergency communications infrastructure and programs, based on coordinated statewide plans, including seamless, ubiquitous, reliable wireless telecommunications networks and enhanced wireless 911 service”).

⁶⁵ See 47 U.S.C. § 942.

authorities and requesting assistance.”⁶⁶ The Commission is further empowered to “promote and enhance public safety by facilitating the rapid deployment of IP-enabled 911 and E-911 services, encourage the Nation’s transition to a national IP-enabled emergency network, and improve 911 and E-911 access to those with disabilities.”⁶⁷ Congress also established a Commission-led Emergency Access Advisory Committee (EAAC) charged with “achieving equal access to emergency services by individuals with disabilities, as a part of the migration to a national Internet protocol-enabled emergency network.”⁶⁸ The Commission has been granted “authority to promulgate regulations to implement the recommendations proposed by the [EAAC], as well as any other regulations, technical standards, protocols, and procedures as are necessary to achieve reliable, interoperable communication that ensures access by individuals with disabilities to an Internet protocol-enabled emergency network, where achievable and technically feasible.”⁶⁹

30. In 2013, pursuant to the Next Generation 9-1-1 Advancement Act of 2012, the Commission submitted to Congress a report containing recommendations for the legal and statutory framework for NG911 services.⁷⁰ This report found that “[t]he consensus view expressed by commenters is that state and local authorities should retain their primary role in the management and development of NG911 by PSAPs, and that general state and local oversight authority over these matters should not be supplanted by the federal government, even in light of the sweeping changes to networks and technology involved in the transition to NG911.”⁷¹ The report also found, however, that “many . . . commenters also call for the federal government to take a more proactive role in leading and coordinating the transition to NG911,” and that “commenters generally support the Commission continuing its role in setting national NG911 policy and providing regulatory oversight consistent with its statutory authority over 911, E911 and NG911.”⁷² The report further recommended that “Congress should consider enacting legislation creating a federal regulatory ‘backstop’ to ensure that there is no gap between federal and state authority (or the exercise thereof) over NG911.”⁷³ While we continue to welcome more specific guidance from Congress regarding the long-term deployment of NG911, we believe that the current risks to 911 described above demand immediate Commission action under existing legal authority.⁷⁴

D. Commission Framework for Reliable 911 Service

31. The Commission provides oversight of 911 communications through several complementary mechanisms, which are reflected in existing rules. First, the Commission requires OSPs to transmit 911 calls, with appropriate location information, to a PSAP.⁷⁵ Second, to reduce the risk of

⁶⁶ Wireless Communications and Public Safety Act of 1999, PL 106–81, 113 Stat 1286 § 3(a) (1999) (codified at 47 U.S.C. § 251(e)(3)).

⁶⁷ New and Emerging Technologies 911 Improvement Act of 2008 (NET 911 Act), PL 110–283, 122 Stat 2620 (2008).

⁶⁸ Twenty-First Century Communications and Video Accessibility Act of 2010, PL 111-260, 124 Stat 2751 at § 106(a) (2010) (CVAA).

⁶⁹ *Id.* at § 106(g).

⁷⁰ See Federal Communications Commission, Legal and Regulatory Framework for Next Generation 911 Services, Report to Congress and Recommendations (2013), available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-319165A1.pdf (NG911 Report).

⁷¹ *Id.* at § 4.1.2.1.

⁷² *Id.*

⁷³ *Id.* at 4.1.2.2.

⁷⁴ See *infra*, Section E.

⁷⁵ See 47 C.F.R. § 64.3001 (“All telecommunications carriers shall transmit all 911 calls to a PSAP, to a designated statewide default answering point, or to an appropriate local emergency authority.”); 47 C.F.R. § 20.18(b) (“CMRS providers subject to this section must transmit all wireless 911 calls without respect to their call validation process to (continued....)”).

911 outages during natural disasters, the Commission requires service providers that aggregate and route 911 calls to PSAPs in each jurisdiction to take reasonable measures to provide reliable service, as evidenced by an annual certification that they have implemented specified best practices or reasonable alternative measures.⁷⁶ Third, the Commission monitors the reliability of 911 networks through mandatory outage reporting requirements that enable statistical analysis of outage trends and inform recommendations to improve network reliability.⁷⁷ When an outage potentially affects a PSAP or other “911 special facility,”⁷⁸ these rules also require certain communications providers to notify the PSAP of outages “as soon as possible”⁷⁹ or within specified time limits.⁸⁰

32. Together, these rules reflect the principle that reliable 911 service must be available to all Americans, at all times and through a broad range of technologies, and that service providers must provide timely notification when 911 outages occur. Each of these rules serves an important function in promoting seamless, ubiquitous, and reliable 911 service nationwide, and we will continue to hold service providers accountable under them. However, changes in technologies and the recent trend in “sunny-day” 911 outages discussed above indicate a potential need for additional targeted action to prevent and mitigate large-scale disruptions in 911 service, and to improve communication and situational awareness among stakeholders.⁸¹ Thus, in this *NPRM*, we do not propose to relieve 911 service providers of existing obligations, but we seek to create new complementary tools that will further reduce the risk of future outages and the duration and impact of any outages that do occur.

33. Accordingly, we set forth core principles to guide the Commission’s 911 governance efforts, and we seek comment on a range of proposals to ensure that governance structure remains robust, effective, and clear to all stakeholders, both today and in the future.

(Continued from previous page) _____
a Public Safety Answering Point.”); 47 C.F.R. § 9.5(b)(2) (“Interconnected VoIP service providers must transmit all 911 calls, as well as ANI and the caller’s Registered Location for each call, to the PSAP, designated statewide default answering point, or appropriate local emergency authority that serves the caller’s Registered Location.”). The Commission has recently expanded 911 requirements to include text-to-911 for Commercial Mobile Radio Service (CMRS) providers and providers of interconnected text messaging applications. *See* 47 C.F.R. § 20.18(n); Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications, Framework for Next Generation 911 Deployment, PS Docket Nos. 11-153, 10-255, *Second Report and Order and Third Further Notice of Proposed Rulemaking*, 29 FCC Rcd. 9846 (2014).⁷⁵

⁷⁶ *See* 47 C.F.R. § 12.4; *911 Reliability Order*, 28 FCC Rcd at 17476.

⁷⁷ *See* 47 C.F.R. Part 4; New Part 4 of the Commission’s Rules Concerning Disruptions to Communications, ET Docket No. 04-35, *Report and Order and Further Notice of Proposed Rulemaking*, 19 FCC Rcd 16830 (2004) (*Part 4 Order*); 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, PS Docket No. 11-82, *Report and Order*, 27 FCC Rcd 2650 (2012) (extending outage reporting requirements to interconnected VoIP providers).

⁷⁸ *See* 47 C.F.R. § 4.5(e).

⁷⁹ *See* 47 C.F.R. §§ 4.9(a)(4) (cable providers); 4.9(c)(2)(iv) (satellite providers); 4.9(e)(5)(wireless providers); 4.9(f)(4) (wireline providers) 4.9(g)(i) (interconnected VoIP providers).

⁸⁰ *See* 47 C.F.R. § 4.9(h) (requiring covered 911 service providers to notify PSAPs within 30 minutes of discovering an outage and follow up with more detailed information within two hours).

⁸¹ For example, the Part 4 rules require information about 911 outages to be provided to the Commission and to affected PSAPs. However, outage reports submitted to the Commission are presumed confidential, *see* 47 C.F.R. § 4.2, and do not address an increasingly apparent need for improved coordination and information-sharing among 911 service providers themselves when a failure of one network component affects multiple providers. We seek comment below on mechanisms to address those and other concerns revealed by recent 911 outages.

III. POLICY STATEMENT

34. It is the policy of the Commission to encourage and support efforts by states and localities to deploy comprehensive end-to-end emergency communications infrastructure and programs, including seamless, ubiquitous, reliable 911 service.⁸² As IP-based 911 service providers transition to architectures that extend beyond the boundaries of any state and implement network changes that may affect quality of service on a regional or national scale, consistent and collaborative governance is not just good governance, but essential to maintaining the vital public benefits of 911. Together with our state and local partners, the Commission has the public safety imperative to oversee each of the increasingly complex component pieces of the nation's 911 infrastructure, and to ensure that service providers within our respective jurisdictions are held fully accountable for providing reliable 911 service to all Americans. Where there are multi-state aspects of the 911 architecture or technology trends that may increase the risk of failure or cause confusion to PSAPs and end-users,⁸³ the Commission must, and will, take a leadership role in resolving such risks and confusion.

35. While we seek comment below on specific proposals designed to address the challenges of the transition to NG911, we believe it would be useful at the outset to articulate the general goals that serve as a framework for these proposals. We start from the proposition that all entities providing 911 communications services, both incumbents and new entrants, occupy a unique position of public trust. Increased innovation and enhanced competition in the 911 ecosystem bring tremendous potential to enhance the functionality and utility of 911, but these transitions must be managed in a manner that maximizes the availability, reliability, and resiliency of the 911 network, and ensures the accountability of all participants in the 911 communications ecosystem. Therefore, we believe that every entity with a role in 911 call completion should be guided by two principles: First, any new elements of 911 architecture or service should have the necessary redundancy and reliability safeguards, along with the appropriate governance mechanisms, to maximize reliability and protect public safety. Second, significant changes in 911 service should be coordinated in a transparent manner with the Commission and with state and local authorities. To the extent that technology transitions and changes in the market for 911 services create real or perceived gaps in the delivery of reliable and resilient 911 service, the Commission will act, in cooperation with state and local partners, to close those gaps and set clear expectations regarding each service.

IV. NOTICE OF PROPOSED RULEMAKING

36. In this *Notice of Proposed Rulemaking*, we first seek comment on specific proposals to advance the principles described above by ensuring that the Commission's 911 rules keep pace with changing technology. We then seek comment on whether it may be appropriate to take further steps, in coordination with state and local authorities, to promote a national governance structure that proactively increases end-to-end accountability and produces measurable results. As we have noted above, covered 911 service providers increasingly are building and operating regional and nationwide IP-based 911 networks that both extend across state boundaries and serve PSAPs in multiple states. We therefore believe such that a comprehensive national approach to the quality and reliability of 911 service is needed, to avoid the risk of confusion and incompatibility that would arise from a patchwork of potentially inconsistent standards.⁸⁴

37. By initiating this rulemaking, we do not intend to impose "one-size-fits-all" mandates on the nation's 911 infrastructure when different states and communities need flexibility to respond to each situation in the way that best suits their particular circumstances. Rather, we seek to ensure that the Commission remains equipped, consistent with its statutory mandates and existing legal authority, with

⁸² See 47 U.S.C. § 615.

⁸³ See *VoIP 911 Order*, 20 FCC Rcd. at 10249, ¶ 8.

⁸⁴ See *id.*

the proper regulatory tools to enforce continued and clear lines of accountability for reliable 911 call completion, including as the nation transitions to an IP-based NG911 architecture. We cannot wait for future and potentially more catastrophic 911 system failures to consider these crucial questions – the stakes are too high.

38. We also emphasize that the purpose of this rulemaking is not to supplant state action. To the contrary, consistent with our statutory mandate under the 911 Act, our goal is to “encourage and support efforts by States to deploy comprehensive end-to-end emergency communications infrastructure,” and to “consult and cooperate with State and local officials” when developing national policies with respect to 911 governance, implementation, and reliability.⁸⁵ We recognize that many decisions regarding 911 deployment, operations, and cost recovery are best made at the state and local level, and continued oversight by states and localities is vital to ensuring that 911 service remains effective and reliable in every community across the country. Our action today is intended to ensure that state and local partners continue to be empowered to fulfill this important oversight responsibility within their jurisdictions, and we seek comment on a variety of ways that the Commission can assist in local, state, and regional efforts to maintain and improve 911 service quality. Thus, we do not intend to interfere with the right of state and local 911 authorities to contract for the services they desire or to determine the best path for deployment of NG911 technologies within their jurisdictions. We also note that, in appropriate circumstances, federal rules may ease burdens on state and local jurisdictions by obviating the need for them to promulgate their own potentially disparate requirements.⁸⁶ We therefore seek comment on the federal-level governance mechanisms described below, as well as ways in which these proposals could assist in state and local efforts to advance similar policy goals.

A. Revisions to Rule 12.4

39. As noted above, the Commission adopted Rule 12.4 based on indications that during the 2012 derecho storm ILECs providing 911 service in affected areas failed to follow established network reliability best practices in three specific areas, which resulted in widespread and prolonged 911 outages.⁸⁷ To address these deficiencies and ensure improved reliability in the future, the rule contains two components: (1) a substantive requirement that “covered 911 service providers shall take reasonable measures to provide reliable 911 service with respect to circuit diversity, central-office backup power, and diverse network monitoring”⁸⁸ and (2) a reporting requirement that such providers certify annually whether they have implemented specified best practices or reasonable alternative measures in each of those substantive areas.⁸⁹ The rule defines “covered 911 service providers” as those that provide specified 911 capabilities, or the functional equivalent, “directly to a PSAP” – typically meaning those entities that provide 911 services pursuant to a contractual agreement with a PSAP or emergency authority.⁹⁰

⁸⁵ See 47 U.S.C. § 615.

⁸⁶ See *911 Reliability Order*, 28 FCC Rcd at 17530-31, ¶ 150.

⁸⁷ *Id.* at 17481-83, ¶¶ 15-21.

⁸⁸ 47 C.F.R. § 12.4(b).

⁸⁹ 47 C.F.R. § 12.4(c).

⁹⁰ 47 C.F.R. § 12.4(a)(4); *911 Reliability Order*, 28 FCC Rcd at 17488-89, ¶ 36. We also note that the Commission has separate reporting requirements for eligible telecommunications carriers (ETCs) under Part 54 of its rules regarding universal service funding. See 47 C.F.R. § 54.202(a)(2) (requiring each ETC to “[d]emonstrate its ability to remain functional in emergency situations, including a demonstration that it has a reasonable amount of back-up power to ensure functionality without an external power source, is able to reroute traffic around damaged facilities, and is capable of managing traffic spikes resulting from emergency situations”); 47 C.F.R. § 54.422(b)(1) (requiring ETCs that receive low-income support to file annual reports including “[d]etailed information on any outage in the prior calendar year” of at least 30 minutes duration that potentially affects at least ten percent of the end users served

(continued....)

40. In the *911 Reliability Order*, the Commission stated that “we are not persuaded that NG911 technologies have evolved to the point that reliability certification rules should apply to entities beyond those that offer core services functionally equivalent to current 911 and E911 capabilities.”⁹¹ It added that “[w]e may, however, revisit this distinction in the future as technology evolves.”⁹² The *911 Reliability Order* contemplated a review of the certification rules in five years, noting that such a review should “include consideration of whether [the rules] should be revised or expanded to cover new best practices or additional entities that provide NG911 capabilities, or in light of our understanding about how NG911 networks may differ from legacy 911 service.”⁹³

41. In light of the multistate 911 outages discussed above and the lessons they provide about 911 network architectures already in use in many parts of the nation, we now believe these questions must be addressed immediately.⁹⁴ The 2012 derecho revealed the dangers of localized legacy 911 infrastructure inadequately prepared to handle an unexpected natural disaster, and in some areas, an unusually high volume of 911 calls.⁹⁵ Recent multi-state 911 outages, by contrast, were not caused by outside factors such as inclement weather, physical damage to network infrastructure, or a loss of commercial power.⁹⁶ They did not reflect failures in disaster preparedness or in the local configuration of central offices and selective routers. Instead, these outages occurred under routine-use conditions, and resulted from the failure of software and databases consolidated in a handful of locations but used to process 911 calls for jurisdictions across the country.⁹⁷ Increasingly complex relationships between carriers, SSPs, sub-contractors, and vendors compounded the difficulty of restoring service due to inadequate communication among affected entities. While other Commission rules establish proactive accountability for transmission of 911 calls to the appropriate PSAP⁹⁸ and timely notification to PSAPs affected by an outage,⁹⁹ Rule 12.4 does not currently address these evolving risks to reliable and resilient 911 service.

42. Accordingly, we propose to expand the scope of entities covered by Rule 12.4 (*i.e.*, the definition of “covered 911 service provider”) to include all entities that provide 911, E911, or NG911 capabilities, such as call routing, automatic location information (ALI), automatic number identification (ANI), location information servers (LIS), text-to-911, or the functional equivalent of those capabilities, regardless of whether they provide such capabilities under a direct contractual relationship with a PSAP

(Continued from previous page) _____
in a designated service area or a “911 special facility,” as defined in 47 C.F.R. § 4.5(e). Nothing in this *NPRM* is intended to modify or replace these requirements for ETCs.

⁹¹ *911 Reliability Order*, 28 FCC Rcd at 17491, ¶ 142.

⁹² *Id.*

⁹³ *Id.* at 17533, ¶ 159.

⁹⁴ See *Multistate 911 Outage Report* at 25 (recommending that “[t]he Commission should conduct further proceedings as necessary to ensure that reliability of 911 service in the United States continues to promote the safety of life and property by maintaining pace with evolving technologies and challenges”).

⁹⁵ See FCC Public Safety & Homeland Security Bureau, *Impact of the June 2012 Derecho on Communications Networks and Services: Report and Recommendations* (Jan. 10, 2013), available at <http://www.fcc.gov/document/derecho-report-and-recommendations> (*Derecho Report*).

⁹⁶ See *Multistate 911 Outage Report* at 1 (observing a recent increase in so-called “sunny day” 911 outages).

⁹⁷ See *id.* at 3 (finding that the April 2014 multistate 911 outage resulted from a preventable coding error in software used to route 911 calls).

⁹⁸ See 47 C.F.R. §§ 64.3001 (telecommunications carriers); 20.18(b) (CMRS providers); 9.5(b)(2) (Interconnected VoIP providers).

⁹⁹ See 47 C.F.R. §4.9.

or emergency authority.¹⁰⁰ This definition would include all entities that provide 911-specific network infrastructure, but only to the extent that they provide specified 911 capabilities. For example, a wireless carrier would be required to certify with respect to any mobile positioning centers (MPCs), gateway mobile location centers (GMLCs) or other databases that it uses to process and route 911 calls, but not with respect to individual cell sites and its call origination network generally.¹⁰¹ This amendment would address 911 network architectures where multiple service providers or sub-contractors provide call routing and ALI/ANI capabilities and ensure that each link in that chain is treated equally under Rule 12.4. We propose that adding these entities would not change the duties of those who already qualify as covered 911 service providers, except with respect to the new certification elements proposed below, or the duties of their agents under existing principles of legal liability.¹⁰² However, we seek comment on the existing duties of the agents and sub-contractors of covered 911 service providers, and on the feasibility of extending certification requirements to such entities.

43. We also propose to expand the range of network reliability practices covered by Rule 12.4 and the corresponding elements of the annual certification based on indications that the current rules may not capture relevant factors in the reliability of existing 911 networks. For example, the April 2014 multistate 911 outage resulted from a software coding error that disrupted routing of 911 calls and inadequate alarm management, which resulted in “significant delays in determining the software fault and restoring 911 service to full functionality.”¹⁰³ Rule 12.4, however, based on the *Derecho Report* and other prior experiences with natural disasters, currently requires certification and reasonable measures to provide reliable service only “with respect to circuit diversity, central-office backup power, and diverse network monitoring.” As technologies evolve, these three categories based on legacy 911 networks may not adequately reflect reasonable measures to provide reliable service, particularly in an NG911 environment.

44. To ensure that Rule 12.4 keeps pace with evolving network architectures and reliability risks, we propose to amend section 12.4(b) to provide that “all covered 911 service providers shall take reasonable measures to provide reliable 911 service.” This obligation would include – but not be limited to – the existing areas of circuit diversity, central-office backup power, and diverse network monitoring. While the current rule 12.4 only addresses reliability with respect to these three specific areas, we believe it would demonstrate better governance for this rule to require covered entities to take reasonable measures generally to ensure the reliability of 911 service, with specific behavior identified within this rule as necessary to add more detail.¹⁰⁴

¹⁰⁰ See Appendix A (proposed Rule 12.4 (4)(i)(D), (E)). We would retain the additional language of Rule 12.4(a)(4)(i)(B), which – in addition to these entities – already includes as a covered 911 service provider any entity that “[o]perates one or more central offices that directly serve a PSAP.” We also would not change Rule 12.4(a)(4)(i)(B)(ii), which excludes from the definition of covered 911 service provider PSAPs or government authorities that provide their own 911 capabilities and entities that merely offer the capability to originate 911 calls where another service provider delivers those calls and associated number or location information to the appropriate PSAP.

¹⁰¹ If a wireless carrier outsources 911 call processing capabilities to a subcontractor, we propose that both the carrier and the subcontractor would be required to certify their respective reasonable measures to maintain reliable 911 service because both entities would provide 911 capabilities specified in the proposed rule. We seek comment on this analysis.

¹⁰² As noted above, while existing Commission rules and legal principles may hold regulatees vicariously liable for the actions of their agents, we believe it would also be helpful for Rule 12.4 to make clear that 911 reliability certification requirements apply independent of a contractual relationship with a PSAP.

¹⁰³ *Multistate 911 Outage Report* at 3.

¹⁰⁴ If the Commission determines to make rule 12.4 a general reasonableness standard, we would intend that this rule supplement any other rules that already contain a requirement to use reasonable measures.

45. We seek comment on additional network reliability practices that should be incorporated into Rule 12.4 and its associated certification requirements. Based on the Bureau's findings with respect to the April 2014 multistate 911 outage and other large-scale disruptions in 911 service described above, we anticipate that one area of particular importance will be the reliability and testing of software and databases used to process 911 calls, including planned maintenance and software upgrades.¹⁰⁵ We also believe that the certification should indicate whether a service provider's IP-based 911 architecture is geographically distributed,¹⁰⁶ load-balanced,¹⁰⁷ and capable of automatic reroutes to backup equipment in the event of a hardware, network, software or database failure. Finally, we believe the network monitoring component of the existing rule should cover not just the physical diversity of monitoring facilities, but also the proper prioritization of critical network alarms.¹⁰⁸ What other measures should be implemented by covered 911 service providers to mitigate the risk of failure and geographic scope of impacts on 911 service? For example, should the certification address factors such as cybersecurity and supply chain risk management?

46. We also believe that Rule 12.4 should reflect and require certification with respect to the duty to take reasonable measures to share information and situational awareness, as appropriate under the circumstances, during disruptions in 911 service.¹⁰⁹ We seek comment on the scope of information and communications that should be reasonably expected from various entities in the 911 ecosystem, including those with direct contractual relationships with PSAPs and those that provide service on a vendor or sub-contractor basis. At a minimum, we believe the certification should indicate whether a covered 911 service provider has a process in place to notify PSAPs of an outage within the timeframes specified in Part 4 of the Commission's rules.¹¹⁰ While this proposal would not change such providers' substantive obligations under Part 4, it would provide assurance that they have taken proactive steps to successfully perform their duties under the rules if the need arises. For example, to ensure that outage notifications are provided swiftly and accurately in the event of an emergency, covered 911 service providers should confirm PSAP contact information and test notification plans periodically. They also might indicate that

¹⁰⁵ See *Multistate 911 Outage Report* at 12 (discussing root causes of the outage).

¹⁰⁶ For example, network architectures utilizing two active databases in different geographic locations, each of which is capable of handling all 911 call traffic in the event of a fault in the other database, will be more reliable and resilient than those that route all calls through a single active database with backup equipment on passive "standby" mode. 911 networks should be "meshed" so that each sub-system can operate with any other available combination of network resources. Resiliency can be further increased by assigning different primary routes for different types of 911 traffic (e.g., wireline, wireless, and VoIP) so that a failure of one gateway into the 911 network would not disrupt 911 service completely.

¹⁰⁷ A 911 network is "load balanced" if call volume is dynamically distributed among all available databases or call processing facilities rather than concentrated in one location. Calls assigned to each database should be automatically rerouted to the other in the event of a fault with the primary route. Furthermore, if two or more PSAPs share the same 911 service provider and rely on each other as a backup PSAP for rerouting of 911 calls, the 911 service provider should consider assigning each PSAP to a different primary routing database.

¹⁰⁸ For example, 911 service providers should have processes in place to send critical alarms to appropriate personnel whenever a substantial proportion of 911 calls are not being processed or completed for more than a few minutes, regardless of cause. This may be accomplished through "peg counts" that compare the number of calls that enter a provider's network to the number of calls that leave the network, or by comparing the number of calls originated to the number of ALI queries returned by the destination PSAPs. Service providers should also consider programming critical alarms to result in the automatic rerouting of 911 calls after reaching a set threshold of time or calls blocked.

¹⁰⁹ See *Multistate 911 Outage Report* at 18 (noting that "many PSAPs in the affected areas stated that they received no notification from ILECs or Intrado about this outage" and that "[w]here information was received, some of those PSAPs believed that it was deficient, and claim that no useful information was imparted to the PSAPs").

¹¹⁰ See 47 C.F.R. § 4.9(h) (requiring covered 911 service providers to notify PSAPs within 30 minutes of discovering an outage and follow up with more detailed information within two hours).

they maintain an outage information email or SMS distribution list that includes all PSAPs in the state(s) they serve and that includes the state emergency management office(s). As noted above, service providers may also be able to detect outages in real time through call counts, ALI queries, and other methods of analyzing network traffic. To what extent should the certification reflect reasonable measures to detect and disseminate such real-time outage information?

47. We seek comment on these proposals and on potential alternative approaches. Are there other topics or practices should be incorporated into “reasonable measures” and annual certification requirements? Should any components of the certification require testing or analysis by an independent third party, or is the certifying entity’s own attestation sufficient? Should the Commission establish standards, best practices, or other mechanisms to promote the reliability of IP-based 911 network elements and processes not currently covered by Rule 12.4? Should such standards be voluntary (*i.e.*, best practices) or mandatory? Should providers be required to report or certify the extent of their compliance with such standards, or should they be required to meet certain standards or performance requirements? Are there instances in an NG911 environment where consensus-based best practices have not yet been established and should be referred to an advisory committee such as the Commission’s Communications Security, Reliability, and Interoperability Council (CSRIC) for further development?¹¹¹ Should we include any limitations on our incorporation of such existing or future standards or practices in our rules? If we include a more general requirement of reliability, should we include additional guidance as to the standards by which the Commission will measure implementation?

B. Ensuring Transparency and Accountability in Connection With Major Changes to Existing 911 Service

48. The functionality of the nation’s 911 networks increasingly depends on complex relationships between service providers and PSAPs, and often among multiple service providers, sub-contractors, and other affiliated entities themselves. While states and localities are well-positioned under our cooperative governance framework to oversee many aspects of these relationships based on the needs of the PSAPs and residents within their borders, critical 911 network infrastructure is increasingly shared among many jurisdictions and beyond the oversight of individual emergency authorities, and more complex in its design and operation. An increasing number of critical 911 capabilities are being provided by one or more non-carrier SSPs and other technical vendors, which, unlike local ILECs, may not have an historical presence in each jurisdiction or a direct contractual relationship with each PSAP that depends on their services for reliable call completion, and are using technologies that may be novel or as yet untested in a particular jurisdiction. This trend will only continue as more and more NG911 functions migrate to the IP “cloud” and are hosted by a broad range of entities in data centers that may be geographically distant from the PSAPs or public that they serve. Accordingly, the end-to-end reliability of a 911 network depends on the sum of its parts and how they function together. We must ensure that this transition process is open and transparent.

1. Major Changes in 911 Service

49. Transparency is essential as the technologies and entities delivering 911 service capabilities evolve over time. In accordance with section 251 of the Communications Act,¹¹² the Commission’s rules require ILECs to provide public notice regarding any network change that will (1) affect a competing service provider’s performance or ability to provide service, (2) affect the ILEC’s interoperability with other service providers, or (3) affect the manner in which customer premises

¹¹¹ See *Multistate 911 Outage Report* at 25 (recommending “that the Commission charge CSRIC with developing and refining a comprehensive set of best practices” with respect to the NG911 transition).

¹¹² 47 U.S.C. 251(c)(5) (requiring telecommunications carriers “to provide reasonable public notice of changes in the information necessary for the transmission and routing of services using that local exchange carrier’s facilities or networks, as well as of any other changes that would affect the interoperability of those facilities and networks”);

equipment is attached to the interstate network,¹¹³ as well as public notice of network changes that “[w]ill result in the retirement of copper loops or copper subloops, and the replacement of such loops with fiber-to-the-home loops or fiber-to-the-curb loops.”¹¹⁴ While the Commission adopted these requirements primarily to “promote[] open and vigorous competition” among local exchange carriers, as contemplated by the Telecommunications Act of 1996,¹¹⁵ network change notifications have also yielded information on certain changes in 911 network architecture that affect interconnection with an ILEC.¹¹⁶ However, an increasing number of covered 911 service providers are not ILECs and are not required to file notifications when changes to their networks may affect 911 connectivity.

50. We therefore propose to require notification to the Commission and the public of major changes in any covered 911 service provider’s network architecture or scope of 911 services that are not otherwise covered by existing network change notification requirements.¹¹⁷ Although parties to individual contracts for 911 services may be aware of major changes in network architecture or in the entities responsible for various 911 functionalities, the public also has a vested interest in understanding changes that may affect its access to 911. Transparency will also promote cooperation and information-sharing among the increasingly diverse range of entities across the 911 ecosystem. We therefore believe that public disclosure of major changes in 911 service is a key step toward increasing accountability when such changes are not initiated at the request of a PSAP or emergency authority or implemented on an emergency basis to mitigate or recover from the effects of an outage.¹¹⁸

51. We seek comment on this proposal. Which 911 service providers should be subject to notification requirements? Should OSPs, ILECs, SSPs, and their sub-contractors each be responsible for reporting major changes in their respective facilities and networks? Or should ILECs and/or SSPs providing 911 services directly to PSAPs be responsible for notification of major changes by their subcontractors and other affiliated entities? We recognize that in many instances changes in 911 network architecture and the entities providing service occur at the request of PSAPs and state or local emergency authorities that desire new or different 911 capabilities. Should such changes be subject to notification requirements, and if so, who should provide the notification? Who should receive the notification? Should the Commission collect and publish such notifications, as it does with wireline network change notifications required under section 251 of the Act and associated Commission rules?¹¹⁹ How could public safety professional organizations such as NENA and APCO facilitate the distribution of such information

¹¹³ 47 C.F.R. § 51.325(a).

¹¹⁴ *Id.* § 51.325(a)(4).

¹¹⁵ See Implementation of the Local Competition Provisions of the Telecommunications Act of 1996, CC Docket No. 96-98, *Second Report and Order and Memorandum Opinion and Order*, 11 FCC Red. 19392, 19471, ¶ 171 (1996).

¹¹⁶ See, e.g., AT&T Network Disclosure ATT20140519L.1 (May 19, 2014), available at <https://ebiznet.att.com/networkreg/#southeast> (announcing that AT&T, on behalf of the Tennessee Emergency Communications Board, is planning to migrate 911 call traffic in the state of Tennessee from a legacy 911 selective router platform to a new, IP-based NG911 network architecture, and noting that “[t]he purpose of this disclosure is to notify all carriers who currently interconnect to any AT&T Tennessee [selective router] that they will need to issue orders to AT&T to provision new connections from their originating networks to two or more of the new AT&T [NG911] ingress points”).

¹¹⁷ This proposal would apply only to changes that do not already trigger network change notification requirements under the Commission’s rules. See 47 C.F.R. § 51.325(a).

¹¹⁸ For example, we do not propose that emergency reroutes to transmit 911 calls to alternate PSAPs or through backup equipment during an outage would be subject to notification requirements, even if such changes affect 911 service in multiple states.

¹¹⁹ See Section 251 Wireline Network Changes, <http://www.fcc.gov/encyclopedia/section-251-wireline-network-changes> (displaying recent notifications filed by ILECs pursuant to 47 C.F.R. §§ 51.325 – 51.335).

to affected PSAPs? To allow sufficient time for public inspection without unnecessarily delaying beneficial network changes, we propose to require notification at least 60 days before major changes in 911 service take effect. We seek comment, however, on whether a shorter – or longer – time period would strike a more appropriate balance.

52. We also seek comment on what changes should be considered “major” for notification purposes. In general, we propose that changes with impact on 911 service in more than a single state should be among the changes considered major. We seek comment on this proposal. Would such an approach lead industry to adopt incremental, state-by-state changes that may not be as efficient? Should we establish thresholds based on factors such as the geography or population affected by a change in the provision of 911 service, regardless of whether their effect is limited to a single state or extends to multiple states? Beyond geographic or population criteria, are there other criteria that for changes in 911 service or network architecture that should trigger a notification requirement? Would it be helpful for an advisory committee such as CSRIC to develop recommendations regarding the types of 911 network changes that should require public notification? Do any existing CSRIC best practices or recommendations provide guidance?

2. Discontinuance or Impairment of Existing 911 Services Essential to Call Completion

53. In addition to proposing public notification of major changes in 911 networks as described above, we believe that additional safeguards are needed where such changes involve discontinuance, reduction or impairment of existing 911 services that are essential to call completion. As with network change notifications, the Commission already has rules requiring common carriers and interconnected VoIP providers to obtain authorization to “discontinue, reduce, or impair service to a community, or part of a community.”¹²⁰ Similarly, we believe that incumbent 911 service providers that have historically taken responsibility for reliable 911 call completion have undertaken a public trust that cannot simply be relinquished at will. While incumbents are entitled to make decisions about their businesses and pursue new and different lines of service, they are not entitled to do so in a manner that endangers the public or leaves stakeholders uninformed with respect to the functioning of the combined network.

54. We therefore propose that covered 911 service providers that seek to discontinue, reduce, or impair existing 911 service in a way that does not trigger already existing authorization requirements should be required to obtain Commission approval.¹²¹ We seek comment on this proposal, and on ways the Commission might address the details of implementation. Are these changes in 911 service of such critical importance that Commission approval should be required before such changes proceed? What processes do states and localities currently have in place to evaluate requests to discontinue, reduce or impair existing 911 service, and how can the Commission support and encourage such processes? Would reliance on states and localities to oversee discontinuance, reduction, or impairment of existing 911 services better serve the policy goals of transparency and accountability?

¹²⁰ See 47 U.S.C. § 214(a); 47 C.F.R. §§ 63.60-63.90. The Commission’s legal authority with respect to 911 provides an independent basis for federal oversight of major changes in the nation’s 911 infrastructure, regardless of whether the associated service providers are carriers, SSPs, or other non-carrier vendors or affiliated entities. See *infra*, Section E.

¹²¹ See Appendix A, proposed Rule 12.5(b). To be clear, nothing in this *Policy Statement and NPRM* would relieve any carrier or interconnected VoIP provider of the requirement to seek permission to discontinue, reduce, or impair service to the extent required by Section 214(a) of the Act and/or the Commission’s implementing rules. We do not, however, intend to create duplicative obligations for entities that are already subject to Section 214(a) and associated authorization requirements. The process proposed here would apply only when entities seeking to discontinue, reduce, or impair existing 911 service are not already required to obtain approval under other existing Commission rules.

55. What actions by an incumbent provider short of a complete discontinuance of 911 service would constitute a reduction or impairment of service for purposes of this requirement? What criteria should the Commission use to evaluate a service provider's request to discontinue, reduce or impair existing 911 service? Which changes in the scope of 911 services offered by an incumbent would be most likely to affect reliable 911 call completion? Should the Commission adopt other requirements specific to incumbent providers seeking to exit lines of 911 service or to outsource elements of that service to third parties? Do CSRIC best practices provide guidance on these questions, and should CSRIC be charged with developing additional best practices or recommendations with respect to the discontinuance, reduction, or impairment of existing 911 services?

56. We do not propose to require public notification or Commission approval under these rules where the discontinuance or reduction of 911 service has been requested or initiated by the PSAP or the responsible state or local emergency authority. We presume that PSAPs and emergency authorities that initiate such changes have the ability to take appropriate steps to safeguard 911 reliability in the affected facilities without Commission intervention.

C. Ensuring Reliability and Accountability of New IP-Based 911 Capabilities and Services

57. Increased innovation and enhanced competition in the NG911 ecosystem hold the potential to enhance the functionality and utility of 911 while providing PSAPs and emergency authorities with greater choice over which services and products they purchase. At the same time, the increasing diversity of entities offering or planning to offer NG911 services increases the challenge of ensuring that all providers of such services will be capable of meeting appropriate standards of reliability and accountability.¹²² It is important that we set clear and consistent expectations with respect to the level of performance that providers of these services will be expected to achieve. Clarifying these obligations is essential to remove uncertainties and barriers to NG911 investment by state, local, and tribal authorities and to maintain public confidence in 911 as the transition to NG911 progresses.

58. Historically, states have overseen the entry of entities providing 911 service through such mechanisms as tariff conditions or issuance of certificates of public convenience and necessity. However, as we have noted above, covered 911 service providers increasingly are building and operating regional and nationwide IP-based 911 networks that both extend across state boundaries and serve PSAPs in multiple states, using less well established technologies. Thus, while states continue to have authority to regulate provision of 911 service within their jurisdictions, these multi-state networks transcend the regulatory authority of any individual state. Moreover, many states have elected not to exercise jurisdiction over IP-based communications, a determination that may operate to restrict their ability to ensure the reliability of 911 service that depends on IP-based technology. We therefore believe that a federal-level process is needed to ensure that there are no regulatory gaps in oversight of providers of new 911 services. This process is not intended to supplant state action; to the contrary, it would complement existing state oversight and could be used to empower state-level action.

59. We propose to require covered 911 service providers that seek to offer new services that affect 911 call completion to certify to the Commission that they have the technical and operational capability to provide reliable 911 service. In addition, to the extent that the new services rely on IP-based networks, associated infrastructure such as servers and data centers, and/or associated software applications, we propose that covered 911 service providers certify that they have conducted a reliability and security risk analysis of the network components, infrastructure, and/or software that they will use to

¹²² See *Multistate 911 Outage Report* at 19 (observing that “new entrants have already begun to enter the market for the provision of key functional services,” and that while “the entry of specialized providers has the potential to promote innovation . . . market forces alone may be insufficient to prevent catastrophic impacts stemming from unchecked aggregation of functions into one or two locations across multiple state boundaries”).

support 911 call completion.¹²³ This proposal would not require Commission approval of new entrants or delay the introduction of innovative new 911 technologies. It would, however, require entities that seek to provide new critical links in 911 call completion to publicly acknowledge their responsibilities and certify their preparedness to implement relevant best practices and comply with existing Commission rules applicable to the 911 capabilities they provide.¹²⁴

60. To what extent do state laws, regulations, or common law tort liability already provide adequate assurances of such qualifications, and is there a need for uniform standards in this regard? Are there quality-of-service requirements under state law that would cover 911-related services, and if so, what entities do they cover? Is there immunity under state law against liability for the provision of 911 related services, or communications services by common carriers or others?¹²⁵ If so, how does such immunity affect incentives among covered service providers and others to ensure that 911 service is reliable? Do the answers to these questions depend upon whether a service is IP-based? How can the Commission facilitate efforts by states and localities to oversee the effective and reliable deployment of new 911 capabilities?

61. If we adopt a certification requirement, which entities should be subject to it, and how should we define the scope of new services that would trigger the need for certification? What information should applicants provide to support their certifications? Should applicants be required to analyze network monitoring capabilities, support for situational awareness, and the ability to share outage information with other stakeholders? Should the certification address issues regarding geographic diversity and redundancy in the network, probabilities of equipment failing due to hardware, network, software and procedural failures, as well as the ability to switch to backup systems? To what extent should the risk analysis include cybersecurity and supply-chain risk assessments? Is it sufficient for service providers to conduct their own analysis or should we require analysis and certification by an independent third party? Would it be helpful for an advisory committee such as CSRIC to develop best practices and recommendations that would serve as a basis for a certification of compliance with best practices for new 911 capabilities and services? For example, should CSRIC be charged with recommending guidelines for the reliability and security risk analysis proposed above? Are there other parts of the communication industry or other industries that have similar certification processes? For example, could the PCI Data Security Standard (PCI DSS) self-certification for entities receiving credit card data provide guidance?¹²⁶

¹²³ This requirement would extend only to IP-based services that are necessary for successful transmission of voice calls and other data to PSAPs. For example, a smart phone “app” that provides the ability to originate calls or text messages to 911 would be subject to certification requirements, while an app that merely enhances or adds value to a smart phone’s existing 911 dialing capabilities would not.

¹²⁴ Because our proposal applies only to new 911 capabilities and is intended to provide public notice and a baseline assurance of reliability, we do not envision the need for a renewal process. Once Covered 911 Service Providers begin offering new capabilities, we believe the annual reliability certification required under Rule 12.4 will be sufficient to ensure continued accountability without additional obligations under this proposal. We seek comment on this issue.

¹²⁵ In its February 2013 report to Congress, the Commission noted the observation of one commenter that immunity afforded to local exchange carriers (which federal law now extends to wireless, interconnected VoIP, and NG911 providers, *see* 47 U.S.C. §§ 615a, 1472), “is often based on telephone company tariffs, which can vary from jurisdiction to jurisdiction or which are being eliminated or replaced or which are tied to a specific . . . technology.” *NG911 Report* at 4.1.5.1. The Commission pointed to NHTSA’s Model State Legislation, which would provide immunity from damage liability for ordinary negligence for any “person involved in the provision of 9-1-1 service who in good faith receives, develops, collects or processes information for the 9-1-1 databases, relays, transfers, operates, maintains or provides 9-1-1 services or system capabilities, or provides emergency 9-1-1 communications or services . . .” *Id.* at 4.1.5.2.

¹²⁶ *See* PCI Security Standards Council, PCI SSC Data Security Standards Overview, https://www.pcisecuritystandards.org/security_standards/ (PCI DSS “provides an actionable framework for

(continued....)

62. As noted above, we do not envision that the federal certification process proposed here would preempt existing state processes for certification of 911 service providers. We believe, however, that states should have the option of adopting the federal certification framework as the basis for state-level governance. We further propose to allow states to enforce federal certification requirements at the state level. We seek comment on this approach. Is there any potential conflict between federal certification for covered 911 service providers and similar state-level processes, and if so, how could such conflicts be minimized? What processes do states and localities currently use to oversee the entry of new 911 service providers, or entities that provide components of 911 service? Do these forms of oversight apply to all entities currently offering one or more components of 911 service, or only to incumbents or some other class of entities? To the extent that states use tariff conditions to regulate the provision of 911 service, what conditions are typically required of new entrants? In states where 911 is not a tariffed service, how do regulators and PSAPs ensure that all entities offering 911 service are both technically capable and committed to public safety?

63. We also do not propose that federal certification would extend to the provision of new call processing services or CPE capabilities that are provisioned by PSAPs themselves under the oversight of state and local governments. Nevertheless, we seek comment on how the Commission can work with state and local partners to ensure that the reliability of PSAP call processing is also maximized. Are there best practices or other measures that PSAPs can take to improve the diversity and robustness of their inbound communications links and the reliability of their CPE? What role should the Commission play with respect to the multi-state deployment and maintenance of new CPE technologies? We note that the Commission recently created a task force on PSAP optimization, which we anticipate will also provide insight regarding PSAP infrastructure, network architecture, and procedures, including call processing.¹²⁷

D. Situational Awareness and Coordination Responsibility During 911 Outages

64. As demonstrated by recent outage trends, the increasing complexity of IP-based 911 network architecture, combined with the increased diversity of entities supporting 911 capabilities, creates potential obstacles to establishing prompt situational awareness and initiating recovery from major 911 outages.¹²⁸ While current Commission rules address outage reporting to the Commission and to affected PSAPs,¹²⁹ the experiences during large-scale 911 outages described above also indicate a need for better coordination and information-sharing among communications providers themselves and any subcontractors or vendors that provide components of the nation's 911 networks. In such outages, restoration of 911 service is likely to be significantly delayed when it is unclear which part of the 911 system has failed and which provider is responsible for repairs. A lack of coordination can also lead to the unacceptable result of multiple entities being involved in an outage but no single entity being able to

(Continued from previous page) _____

developing a robust payment card data security process – including prevention, detection and appropriate reaction to security incidents. Tools to assist organizations validate their PCI DSS compliance include Self Assessment Questionnaires”).

¹²⁷ See Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications; Framework for Next Generation 911 Deployment, *Second Report and Order*, PS Docket Nos. 11-153, 10-255 (rel. Aug. 13, 2014) at ¶¶ 79-80; FCC Seeks Nominations by November 7, 2014 for Membership on New Task Force on Optimal Public Safety Answering Point Architecture, *Public Notice*, DA 14-1481 (Oct. 10, 2014).

¹²⁸ See *Multistate 911 Outage Report* at 21 (finding a “lack of clear lines of communication” between entities involved in the April 2014 multistate 911 outage and noting that “[a]ll entities in the chain of end-to-end 911 service must give serious consideration to ensuring that information about alarms associated with critical physical and logical functionalities is shared among such entities along the 911 call chain”).

¹²⁹ See 47 C.F.R. § 4.9.

provide timely and comprehensive information about the outage to the PSAPs and public that they serve.¹³⁰

65. To address these concerns, we believe that more needs to be done to address gaps in situational awareness and coordination when large-scale 911 outages affect multiple jurisdictions and service providers. First, effective information sharing is key when diagnosing and repairing problems that may span multiple providers' networks or originate with one provider but affect many others. Second, in the increasingly diverse NG911 ecosystem, it will be more and more difficult for PSAPs and 911 service providers to coordinate an effective and timely response to outages without a central clearinghouse for obtaining and disseminating critical information. Accordingly, we propose to clarify responsibility for situational awareness and coordination among 911 service providers, sub-contractors, and other affiliated entities during disruptions in 911 service. While it may not be technically or economically feasible for a single entity to monitor, control, or repair every segment of a 911 network from caller to PSAP, it would be helpful for one covered 911 service provider in each jurisdiction to perform a triage function to mitigate the duration and impact of outages.

66. To establish a clearinghouse mechanism for critical information during major 911 outages and other significant degradations in service,¹³¹ we propose to establish a class of covered 911 service providers that would assume primary responsibility for situational awareness and information sharing. These entities – which we propose to call “911 Network Operations Center (NOC) providers” – would be responsible for monitoring their networks to detect disruptions or degradations in 911 service, and for affirmatively communicating relevant information, as appropriate, to other stakeholders, including OSPs, SSPs, vendors, PSAPs, state emergency management offices, and the Commission's Operations Center. As a corollary to this proposal, 911 NOC providers would be empowered to obtain relevant information concerning outages from other covered 911 service providers, who in turn would be required to provide information in response to the 911 NOC provider's requests. 911 NOC providers would then coordinate with other stakeholders to collect and distribute information regarding the impact of outages on all affected portions of the network from call origination to completion.

67. We propose that the role of 911 NOC provider for each jurisdiction should be assigned to the entity responsible for transport of 911 traffic to the PSAP or PSAPs serving that jurisdiction. In many cases, we expect that this role would be assumed by the incumbent LEC, because, as noted above, ILECs have historically provided transport of 911 traffic to PSAPs and have thereby occupied the best position to maintain comprehensive situational awareness, even as SSPs and vendors have come to provide component pieces of those networks. Nevertheless, as 911 networks evolve, other entities may take on the 911 transport responsibilities that ILECs have historically provided. For example, in an NG911 environment, the 911 transport function may be performed by an ESINet provider that receives 911 traffic from originating service providers and directs the traffic to PSAPs served by the ESINet. In such cases, we envision that the ESINet provider would assume the 911 NOC provider role. We seek comment on this approach. Should ILECs, ESINet providers, and other entities responsible for 911 transport be the 911 NOC providers bearing primary responsibility for maintaining situational awareness, sharing information, and coordinating outage recovery among other affected providers? Are there situations where more than one entity can reasonably be described as being responsible for aspects of transport of 911 traffic to the PSAP or PSAPs serving a jurisdiction? In such situations, which entity would be best suited to fill the 911 NOC provider role?

¹³⁰ See *Multistate 911 Outage Report* at 21 (“Despite the fact that Intrado owned and operated the software at fault, Intrado suggests that it is not responsible for presenting a coherent picture of what happened.”)

¹³¹ We intend this proposal to extend to outages resulting in a complete loss of 911 service as well as other situations, such as emergencies resulting in unusually high call volume or cybersecurity events, that may impact service quality without causing a complete loss of connectivity. We seek comment on the scope of circumstances that should be considered an outage or significant degradation in service for purposes of this requirement.

68. Under this framework, we anticipate the need for only one 911 NOC provider in each jurisdiction; indeed, the 911 NOC provider's role as a clearinghouse for situational awareness will be most effective with a single point of contact for relevant information. We also emphasize that the proposed responsibilities of 911 NOC providers during an outage would be limited in scope. For instance, 911 NOC providers would not be expected to have omniscient situational awareness of the status of 911 network components outside their control¹³² except to the extent they are empowered to obtain such information from other parties or through their own network monitoring processes. Instead, 911 NOC providers would serve as a hub for the collection, aggregation, and communication of available information among covered 911 service providers and other affected stakeholders to mitigate the impact of outages and support rapid restoration of service. In addition, while 911 NOC providers would be tasked with obtaining and disseminating outage information, they would not be legally responsible for adverse consequences resulting from outages attributable to failures of network components outside their control, or for remediating or repairing such failures.

69. We do not intend these proposals to supersede or replace existing outage reporting requirements under Part 4 of the Commission's rules. Thus, we begin with the assumption that all parties covered by existing Part 4 requirements would continue to be required to report outages to the Commission that meet the Part 4 outage thresholds, and requirements for certain service providers to notify PSAPs and other "911 Special Facilities" of outages affecting 911 service would continue to apply independently of any action taken in this proceeding.¹³³ We note, however, that the Commission has historically relied on mandatory outage reporting to gather statistical information on trends in communications reliability to assess the effectiveness of best practices and provide policy guidance on efforts to increase network reliability.¹³⁴ While closely related, the need to share information and situational awareness among service providers affected by an outage may pose different challenges requiring different oversight mechanisms. We therefore seek comment on the alternative proposal of whether certain obligations currently in Part 4 would be better assigned to 911 NOC providers under the framework proposed above. For example, should current responsibilities to notify PSAPs of outages affecting 911 service be incorporated into the information-sharing responsibilities of the 911 NOC provider, rather than the outage-reporting responsibilities of multiple service providers under current Rule 4.9?¹³⁵ Should the Commission consider any other changes to Part 4 in light of the responsibilities of 911 NOC providers proposed here?

70. We also seek comment on processes and mechanisms that 911 NOC providers and other covered 911 service providers could use to carry out their situational awareness and coordination responsibilities proposed here. As described above with respect to reliability certification requirements, service providers may be able to detect outages in real time by tracking the number of 911 calls that enter and exit their networks, an increase in call failure rates, positioning failure rates, or the number of calls that result in an ALI or LIS query from the destination PSAP. Service providers should have alarms configured to bring such discrepancies to the attention of appropriate personnel. To what extent should 911 NOC providers and other covered 911 service providers be expected to share information in real time

¹³² 911 NOC providers would be responsible for network components within the control of their agents, contractors and sub-contractors, or others acting on their behalf. *See supra*, ¶ 18 (noting how the Commission has long held that licensees and other regulatees are responsible for the acts and omissions of their employees and independent contractors).

¹³³ *See* 47 C.F.R. § 4.9.

¹³⁴ *See* New Part 4 of the Commission's Rules Concerning Disruptions to Communications, ET Docket No. 04-35, *Report and Order and Further Notice of Proposed Rulemaking*, 19 FCC Rcd 16830, 16838, ¶ 12 (2004) (noting that "[s]ervice disruption reporting has also permitted us to assess trends in wireline reliability and determine the extent to which our policies need modification").

¹³⁵ *See* 47 C.F.R. §§ 4.9(a)(4) (cable providers); 4.9(c)(2)(iv) (satellite providers); 4.9(e)(5) (wireless providers); 4.9(f)(4) (wireline providers) 4.9(g)(i) (interconnected VoIP providers); 4.9(h) (covered 911 service providers).

about call counts and alarms using standardized network management interfaces or other mechanisms?¹³⁶ or other mechanisms? Should CSRIC be charged with developing recommendations on these topics?

71. How can the Commission facilitate the real-time exchange of information by leveraging technologies such as machine-readable data? Should the Commission require 911 NOC providers or other covered 911 service providers to transmit high-level data on the status of their networks¹³⁷ to a centralized “dashboard” allowing users to quickly identify disruptions in any portion of their 911 networks? Who should be given access to such data, and how can the Commission ensure that privacy and confidentiality are protected? Alternatively, should 911 NOC providers be required to maintain a Web page that provides key information on the status of their 911 networks? What information should be included, and should such Web pages be available to the public, or only to PSAPs and other covered 911 service providers?

72. How can the Commission support and empower 911 NOC providers and other covered 911 service providers to share information under the framework proposed above? One model for improved situational awareness that has been developed in the communications sector is the Information Sharing and Analysis Center (ISAC), a public-private partnership overseen by the U.S. Department of Homeland Security National Coordinating Center for Communications (NCC).¹³⁸ Could a similar model be applied to the 911 ecosystem? Which entities should be eligible to participate, and should certain entities, such as NOC providers, be required to participate? Should the Commission facilitate improved communication by maintaining a centralized database of contact information for PSAPs and state emergency offices, which would allow 911 NOC providers and other covered 911 service providers to compile and update distribution lists for outage notification and recovery? Should the Commission serve as a hub for compilation and distribution of any other information? What role could advisory committees such as CSRIC play?

73. We also seek comment on issues that could affect the nature and scope of a NOC provider’s responsibility for information gathering and dissemination. For example, should the scope of information that the NOC provider is responsible for gathering and disseminating vary depending on where in the call completion process a 911 outage has occurred? If so, what should the 911 NOC provider’s responsibility be? To what extent should 911 NOC providers be responsible for addressing cybersecurity risks in 911 networks and sharing information with other stakeholders in the event of a cyber attack? What information should other covered 911 service providers that experience the effects of an outage be expected to communicate back to the 911 NOC provider?

74. Where a PSAP is served by more than one covered 911 service provider (*e.g.*, where a PSAP has a direct contractual relationship with an ILEC that sub-contracts with an SSP or other affiliated entity for 911 capabilities), should the parties be required to designate specific support roles? Beyond the proposal that primary 911 NOC support is best provided by the 911 transport provider, should the Commission require covered 911 service providers to designate a hierarchy of responsibility for such support or encourage PSAPs and providers to negotiate their own agreements? Or should such determinations be made at the state or local level through tariff conditions or requests for proposals for

¹³⁶ For example, the RFC 4780 standard defines a Management Information Base (MIB) for monitoring call counts, using the widely used Simple Network Management Protocol (SNMP). It may be appropriate to define additional MIBs for monitoring LIS and other key NG911 elements. See Internet Engineering Task Force (IETF), Management Information Base for the Session Initiation Protocol (SIP) RFC 4780, *available at* <https://datatracker.ietf.org/doc/rfc4780/>.

¹³⁷ This data might be as simple as whether a provider’s network is “up” or “down,” or it might include more comprehensive metrics such the number of calls received, or additional diagnostic information. We seek comment on the scope of information that should be shared.

¹³⁸ See U.S. Department of Homeland Security, National Coordinating Center for Communications, <http://www.dhs.gov/national-coordinating-center-communications> (last accessed Sept. 11, 2014).

911 service? What information should covered 911 service providers that are not NOC providers be expected to share with each other?

75. Are there legal or regulatory barriers that currently prevent or discourage 911 service providers, as well as their sub-contractors and other affiliated entities, from sharing information during a 911 outage?¹³⁹ What are the specific laws, regulations, or contractual provisions that would preclude such information-sharing, and how can the Commission address those barriers in order to improve efficient, privacy-protective information sharing and situational awareness? Are there issues of legal liability for disclosing customer information that should be addressed as part of the Commission's efforts in this regard? Should the Commission extend liability protections already afforded to certain entities¹⁴⁰ to additional participants in the 911 ecosystem?

E. Legal Authority

76. The Communications Act of 1934 established the FCC, in part, “for the purpose of promoting safety of life and property through the use of wire and radio communication.”¹⁴¹ Beyond that general mandate, Congress has repeatedly and specifically endorsed a role for the Commission in the nationwide implementation of advanced 911 capabilities. The Wireless Communications and Public Safety Act of 1999 (911 Act) directed the Commission to “designate 911 as the universal emergency telephone number within the United States for reporting an emergency to appropriate authorities and requesting assistance.”¹⁴² It also directed the Commission to “encourage and support efforts by States to deploy comprehensive end-to-end emergency communications infrastructure and programs, based on coordinated statewide plans, including seamless, ubiquitous, reliable wireless telecommunications networks and enhanced wireless 911 service.”¹⁴³ The New and Emerging Technologies 911 Improvement Act of 2008 (NET 911 Act) further affirmed the Commission's authority to require interconnected VoIP providers to offer 911 service.¹⁴⁴ The Twenty-First Century Communications and Video Accessibility Act of 2010 (CVAA) also advanced the Commission's implementation of technologies such as text-to-911 by granting authority to promulgate “regulations, technical standards, protocols, and procedures . . . necessary to achieve reliable, interoperable communication that ensures access by individuals with disabilities to an Internet protocol-enabled emergency network, where achievable and technically feasible.”¹⁴⁵ Together, and in light of the series of 911 outages described above extending across multiple jurisdictions, we believe these provisions authorize – and indeed require – the Commission to take a leadership role, in cooperative partnership with states and localities, in promoting the continued availability and reliability of 911 services nationwide.

¹³⁹ See *Multistate 911 Outage Report* at 22 (“Intrado suggests that it is contractually precluded from providing the Commission or PSAPs with a clear understanding of what happened, adding that its business units are under contract to varying service providers and government agencies, and that ‘those contracts are strictly honored.’”).

¹⁴⁰ See 47 U.S.C. § 615(a); 47 U.S.C. § 1472.

¹⁴¹ 47 U.S.C. § 151.

¹⁴² Wireless Communications and Public Safety Act of 1999, PL 106–81, 113 Stat 1286 § 3(a) (1999) (codified at 47 U.S.C. § 251(e)(3)).

¹⁴³ *Id.* at § 3(b) (codified at 47 U.S.C. § 615).

¹⁴⁴ New and Emerging Technologies 911 Improvement Act of 2008 (NET 911 Act), PL 110–283, 122 Stat 2620 (2008); see also 47 U.S.C. § 615a-1(a), (c)(1)(B) (requiring “each IP-enabled voice service provider to provide 9-1-1 service and enhanced 9-1-1 service to its subscribers in accordance with the requirements of the Federal Communications Commission” and directing the Commission to “take into account any technical, network security, or information privacy requirements that are specific to IP-enabled voice services” when promulgating regulations under the NET 911 Act).

¹⁴⁵ Twenty-First Century Communications and Video Accessibility Act of 2010, PL 111-260, 124 Stat 2751 § 106(g) (2010) (CVAA) (codified at 47 U.S.C. § 615c(g)).

77. To the extent that 911 service providers are common carriers, the Commission also has based 911 reliability requirements on section 201(b) of the Communications Act,¹⁴⁶ which requires the “practices” of common carriers to be “just and reasonable,” and on section 214(d),¹⁴⁷ which provides that a common carrier must “provide itself with adequate facilities for the expeditious and efficient performance of its service as a common carrier.”¹⁴⁸ Where 911 service requirements affect wireless carriers, the Commission also has relied on its Title III authority to “[p]rescribe the nature of the service to be rendered,”¹⁴⁹ and more generally, “to manage spectrum . . . in the public interest.”¹⁵⁰

78. With respect to proposals to promote transparency and public notification for changes in 911 service, we note that Section 218 of the Act authorizes the Commission to “inquire into the management of the business of all carriers,” and to obtain from such carriers and from persons directly or indirectly under their control “full and complete information necessary to enable the Commission to perform the duties and carry out the objects for which it was created.”¹⁵¹ Section 251(c)(5) of the Act also requires each incumbent local exchange carrier to “provide reasonable public notice of changes in the information necessary for the transmission and routing of services,” or “other changes that would affect the interoperability of [its] facilities and networks.”¹⁵² Furthermore, Section 4(o) of the Act states that “[f]or the purpose of obtaining maximum effectiveness from the use of radio and wire communications in connection with safety of life and property,” the Commission “shall investigate and study all phases of the problem and the best methods of obtaining the cooperation and coordination of these systems.”¹⁵³ The Commission also has authority, under the New and Emerging Technologies 911 Improvement Act of 2008, to “compile . . . information concerning 9-1-1 and enhanced 9-1-1 elements, for the purpose of assisting IP-enabled voice service providers in complying with this section.”¹⁵⁴ Thus, as part of a cooperative governance structure for 911, the Commission is authorized to gather and disseminate information from carriers and other regulatees for the purpose of ensuring effective public safety communications. We seek comment on the application of these provisions to proposals in this *NPRM*.

79. As the Commission concluded in the *911 Reliability Order*, “[i]n light of these express statutory responsibilities, regulation of additional capabilities related to reliable 911 service, both today and in an NG911 environment, would be well within Commission’s . . . statutory authority.”¹⁵⁵ That order also committed to review the rules established therein, “in light of our understanding about how NG911 networks may differ from legacy 911 service,” and based on such factors as “outage reporting trends” and “adoption of NG911 capabilities on a nationwide basis.”¹⁵⁶ Accordingly, we believe that the

¹⁴⁶ 47 U.S.C. § 201(b).

¹⁴⁷ 47 U.S.C. § 214(d).

¹⁴⁸ See *911 Reliability Order*, 28 FCC Rcd. at 17529, ¶ 149.

¹⁴⁹ 47 U.S.C. § 303(b). See also *id.* §§ 303(r), 316; *911 Reliability Order*, 28 FCC Rcd. at 17529, ¶ 149; Facilitating the Deployment of Text-to-911 & Other Next Generation 911 Applications, PS Docket Nos. 11-153, 10-255, *Report and Order*, 28 FCC Rcd. 7556, 7587-7605, ¶¶ 88-140 (2013).

¹⁵⁰ *Cellco Partnership v. FCC*, 700 F.3d 534, 541-42 (D.C. Cir. 2012) (citing 47 U.S.C. § 303(b)).

¹⁵¹ 47 U.S.C. § 218. See also 47 U.S.C. 303(j) (authorizing the Commission to issue rules and regulations requiring wireless licensees to keep records of “programs, transmissions of energy, communications, or signals”).

¹⁵² 47 U.S.C. § 251(c)(5).

¹⁵³ 47 U.S.C. § 154(o).

¹⁵⁴ 47 U.S.C. § 615a-1(g).

¹⁵⁵ *911 Reliability Order*, 28 FCC Rcd at 17529, ¶¶ 148-150 (citing 47 U.S.C. §§ 251(e), 201(b), § 214(d), and other provisions). See also *Nuvio Corp. v. FCC*, 473 F.3d 302, 312 (D.C. Cir. 2006) (Kavanaugh, J., concurring) (recognizing “[t]he broad public safety and 911 authority Congress has granted the FCC”).

¹⁵⁶ *911 Reliability Order*, 28 FCC Rcd at 17533 ¶ 159.

Commission would have ample legal authority to adopt any or all of the proposals discussed above, consistent with our longstanding policy of cooperation with state and local authorities. We seek comment on this analysis. In particular, we seek comment from state and local regulators and emergency authorities regarding the appropriate balance of federal, state, and local authority in each of the proposals described above.

80. To the extent that any of the proposals herein affect entities that are not subject to specific statutory authority, we also believe that their adoption would be that “reasonably ancillary to the Commission’s effective performance of its statutorily mandated responsibilities.”¹⁵⁷ Whether or not the increasingly diverse range of entities providing 911 services are common carriers or Commission licensees, they nevertheless have undertaken to provide a critical public safety communications service that is within our general jurisdiction to “promot[e] safety of life and property through the use of wire and radio communication.”¹⁵⁸ In light of the record of recent events leading to significant multistate 911 outages, we believe such proposals would be reasonably ancillary to our fulfillment of the specific statutory mandates to ensure reliable and resilient 911 service across different technologies, as discussed above. We seek comment on this analysis and any other sources of legal authority for the proposals in this *NPRM*.

V. PROCEDURAL MATTERS

A. *Ex Parte* Presentations

81. The proceedings initiated by this *Notice of Proposed Rulemaking* shall be treated as “permit-but-disclose” proceedings in accordance with the Commission’s *ex parte* rules.¹⁵⁹ Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must: (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made; and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter’s written comments, memoranda, or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission’s *ex parte* rules.

¹⁵⁷ See 47 U.S.C. § 154(i) (“The Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions.”); *Am. Library Ass’n v. FCC*, 406 F.3d 689, 691-92 (D.C. Cir. 2005) (“The Commission . . . may exercise ancillary jurisdiction only when two conditions are satisfied: (1) the Commission’s general jurisdictional grant under Title I covers the regulated subject and (2) the regulations are reasonably ancillary to the Commission’s effective performance of its statutorily mandated responsibilities.”).

¹⁵⁸ 47 U.S.C. § 151.

¹⁵⁹ 47 C.F.R. §§ 1.1200 *et seq.*

B. Comment Filing Procedures

82. Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments in response to this *Notice of Proposed Rulemaking* on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). See *Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: <http://fjallfoss.fcc.gov/ecfs2/>.
- Paper Filers: Parties that choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number.

Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

- All hand-delivered or messenger-delivered paper filings for the Commission's Secretary must be delivered to FCC Headquarters at 445 12th St., SW, Room TW-A325, Washington, DC 20554. The filing hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.
- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12th Street, SW, Washington DC 20554.

C. Accessible Formats

83. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (TTY).

D. Regulatory Flexibility Act

84. As required by the Regulatory Flexibility Act of 1980, *see* 5 U.S.C. § 604, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities of the policies and rules addressed in this document. The IRFA is set forth in Appendix B. Written public comments are requested in the IRFA. These comments must be filed in accordance with the same filing deadlines as comments filed in response to this *Notice of Proposed Rulemaking* as set forth on the first page of this document, and have a separate and distinct heading designating them as responses to the IRFA.

E. Paperwork Reduction Act

85. This *Notice of Proposed Rulemaking* contains proposed new information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and OMB to comment on the information collection requirements contained in this document, as required by PRA. In addition, pursuant to the Small Business Paperwork Relief Act of

2002,¹⁶⁰ we seek specific comment on how we might “further reduce the information collection burden for small business concerns with fewer than 25 employees.”¹⁶¹

F. Congressional Review Act

86. The Commission will send a copy of this *Policy Statement and Notice of Proposed Rulemaking* in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act (CRA), *see* 5 U.S.C. § 801(a)(1)(A).

VI. ORDERING CLAUSES

87. Accordingly, IT IS ORDERED, pursuant to Sections 151, 154(i), 154(j), 154(o), 155(c), 201(b), 214(d), 218, 219, 251(e), 301, 303(b), 303(g), 303(j), 303(r), 332, 403, 615, 615a, 615c, 621(b)(3), and 621(d) of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154(i), 154(j), 154(o), 155(c), 201(b), 214(d), 218, 219, 251(e), 301, 303(b), 303(g), 303(j), 303(r), 332, 403, 615, 615a, 615c, 621(b)(3), and 621(d), that this *Policy Statement and Notice of Proposed Rulemaking* in PS Docket Nos. 14-193 and 13-75 IS ADOPTED.

88. IT IS FURTHER ORDERED that the Commission’s Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this *Policy Statement and Notice of Proposed Rulemaking*, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

¹⁶⁰ Pub. L. No. 107-198.

¹⁶¹ 44 U.S.C. § 3506(c)(4).

APPENDIX A

Proposed Rules

Part 12 of Title 47 of the Code of Federal Regulations is proposed to be amended as follows:

PART 12 – RESILIENCY, REDUNDANCY, AND RELIABILITY OF COMMUNICATIONS**1. Revise the authority for Part 12 to read as follows:**

Authority: 47 U.S.C. §§ 151, 154(i), 154(j), 154(o), 155(c), 201(b), 214(d), 218, 219, 251(e), 301, 303(b), 303(g), 303(j), 303(r), 332, 403, 615, 615a, 615c, 621(b)(3), and 621(d).

2. Revise paragraphs (a)(4), (b), and (c)(3) of § 12.4 to read as follows:

§ 12.4 Reliability of Covered 911 Service Providers

(a) * * *

(4) *Covered 911 Service Provider.*

i. Any entity that:

(A) Provides call routing, automatic location information (ALI), automatic number identification (ANI), location information services (LIS), text-to-911, or any other capability required for delivery of 911, E911, or NG911, or the functional equivalent of any of those capabilities, to a public safety answering point (PSAP), statewide default answering point, or appropriate local emergency authority as such entities are defined in 47 C.F.R. § 64.3000(b), whether directly or indirectly as a contractor or agent to any other entity; and/or

(B) Operates a central office that directly serves a public safety answering point (PSAP), statewide default answering point, or appropriate local emergency authority as such entities are defined in 47 C.F.R. § 64.3000(b). For purposes of this section, a central office directly serves a PSAP, statewide default answering point, or appropriate local emergency authority if it hosts a selective router or the functional equivalent, hosts an ALI/ANI database or the functional equivalent, or is the last service-provider facility through which a 911 trunk or administrative line passes before connecting to a PSAP, statewide default answering point, or appropriate local emergency authority.

ii. The term “Covered 911 Service Provider” shall not include:

(A) PSAPs or governmental authorities to the extent that they provide 911, E911, or NG911 capabilities; or

(B) Communications providers that solely originate voice calls or text messages to 911 but do not provide any of the capabilities or services described in subparagraph (i) of this subsection.

* * *

- (b) *Provision of Reliable 911 Service.* All Covered 911 Service Providers shall take reasonable measures to provide reliable 911 service. Performance of the elements of the Certification set forth in subsections (c)(1)(i), (c)(2)(i), (c)(3)(i), (c)(4)(i), and (c)(5)(i) below shall be deemed to satisfy the requirements of this subsection (b). If a Covered 911 Service Provider cannot certify that it has performed a given element, the Commission may determine that such provider nevertheless satisfies the requirements of this subsection (b) based upon a showing in accordance with subsection (c) that it is taking alternative measures with respect to that element that are reasonably sufficient to mitigate the risk of failure, or that one or more certification elements are not applicable to its network.

* * *

- (c) * * *

(3) *Network Monitoring.*

- (i) A Covered 911 Service Provider shall certify whether it has, within the past year:
- (A) Conducted Diversity Audits of the Aggregation Points that it uses to gather network monitoring data in each 911 Service Area;
 - (B) Conducted Diversity Audits of Monitoring Links between Aggregation Points and NOCs for each 911 Service Area in which it operates; and
 - (C) Implemented Physically Diverse Aggregation Points for network monitoring data in each 911 Service Area and Physically Diverse Monitoring Links from such aggregation points to at least one NOC.
 - (D) Established appropriate alarms for network failures that would be reasonably likely to result in a disruption of 911 service within a 911 Service Area, and procedures designed to ensure that such alarms quickly bring such network failures to the attention of appropriate personnel.
- (ii) If a Covered 911 Service Provider has not implemented all of the elements in subsection (c)(3)(i) above, it must certify with respect to each such 911 Service Area:
- (A) Whether it has taken alternative measures to mitigate the relevant risk, or is taking steps to remediate any vulnerabilities that it has identified with respect thereto, in which case it shall provide a brief explanation of such alternative measures or such remediation steps, the date by which it anticipates such remediation will be completed, and why it believes those measures are reasonably sufficient to mitigate such risk; or
 - (B) Whether it believes that one or more of the requirements of this subsection are not applicable to its network, in which case it shall provide a brief explanation of why it believes any such requirement does not apply.

* * *

3. Add paragraphs (a)(12), (a)(13), (a)(14), (c)(4) and (c)(5) of § 12.4 to read as follows:

- (a) * * *

(12) *Geographically distributed.* For purposes of this section, 911 network architecture is

geographically distributed if all calls on the 911 network can be routed through more than one database or call processing facility in more than one geographic location.

- (13) *Load balanced.* For purposes of this section, 911 network architecture is load balanced if call volume is dynamically distributed among multiple active databases or call processing facilities rather than concentrated in one active location.
- (14) *Situational awareness.* For purposes of this section, situational awareness means the ability to detect disruptions or degradations in 911 service, to assess the scope and impact of such disruptions or degradations in 911 service, and to share information as appropriate to mitigate and resolve such impacts.

* * *

(c) * * *

(4) *Database and Software Configuration and Testing*

- (i) A Covered 911 Service Provider shall certify whether it has, within the past year:
- (A) Implemented reasonable measures to ensure that any Internet Protocol (IP)-based architecture used to provide 911, E911, or NG911 capabilities defined in subsection 12.4(a)(4)(i) of this section is geographically distributed, load balanced, and capable of automatic reroutes in the event of a software or database failure.
 - (B) Implemented reasonable measures to ensure that any software or database used by the Covered 911 Service Provider to provide 911, E911, or NG911 capabilities such as call routing, automatic location information (ALI), automatic number identification (ANI), location information services (LIS), text-to-911, or the functional equivalent of those capabilities, is designed, configured, and tested to ensure reliable operation.
 - (C) Implemented reasonable measures to maintain continuity of 911 service during planned maintenance and/or updates to any software or database used to provide 911, E911, or NG911 capabilities.
- (ii) If a Covered 911 Service Provider has not implemented all of the elements in subsection (c)(4)(i) above, it must certify:
- (A) Whether it has taken alternative measures to mitigate the risk of a hardware, network, software, database, or other failure or is taking steps to remediate any issues that it has identified with respect thereto, in which case it shall provide a brief explanation of such alternative measures or such remediation steps, the date by which it anticipates such remediation will be completed, and why it believes those measures are reasonably sufficient to mitigate such risk; or
 - (B) Whether it believes that one or more of the requirements of this subsection are not applicable to its network, in which case it shall provide a brief explanation of why it believes any such requirement does not apply.

(5) *Situational Awareness and Information Sharing*

- (i) A Covered 911 Service Provider shall certify whether it has, within the past year:
 - (A) Implemented reasonable measures to maintain real-time situational awareness regarding the operational status of 911, E911, or NG911 service throughout any portion(s) of the 911 network that it owns, leases, or otherwise operates or controls or as to which it otherwise provides any of the capabilities or services described in subsection 12.4(a)(4)(i)(A) of this section.
 - (B) Implemented reasonable measures to share appropriate information with PSAPs and other Covered 911 Service Providers in the event of a disruption of 911 E911, or NG911 service, including, at a minimum, the information required under Part 4 of the Commission's rules and under section 12.7 of this Part 12.
- (ii) If a Covered 911 Service Provider has not implemented all of the elements in subsection (c)(5)(i) above, it must certify:
 - (A) Whether it has taken alternative measures to mitigate the risk of inadequate situational awareness and information sharing or is taking steps to remediate any issues that it has identified, in which case it shall provide a brief explanation of such alternative measures or such remediation steps, the date by which it anticipates such remediation will be completed, and why it believes those measures are reasonably sufficient to mitigate such risk; or
 - (B) Whether it believes that one or more of the requirements of this subsection are not applicable to its network, in which case it shall provide a brief explanation of why it believes any such requirement does not apply.

* * * * *

4. Add section 12.5 to read as follows:

§ 12.5 Transparency and Accountability in Connection With Major Changes in 911 Service

- (a) *Major Changes in 911 network architecture and services.* A Covered 911 Service Provider, as defined in section 12.4(a)(4), seeking to make major changes in its 911 network architecture and services shall file a public notification under this section, except as provided under subsections (a)(3), (a)(4), and (a)(5).

- (1) For purposes of this section, the following actions by a Covered 911 Service Provider constitute major changes in 911 network architecture and services:

- i) A change in 911 network architecture that affects the primary geographic routing or logical processing of voice calls, automatic location information (ALI), automatic number identification (ANI), location information services (LIS), text-to-911, or functionally equivalent capabilities, to public safety answering points (PSAPs), statewide default answering points, or appropriate local emergency authorities in more than one state;
- ii) A change in 911 network architecture that affects the availability of backup routing or processing capabilities for voice calls, ALI, ANI, LIS, text-to-911, or functionally equivalent capabilities, to PSAPs, statewide default answering points, or appropriate local

- emergency authorities in more than one state; or
- iii) A change in the allocation of primary responsibility with respect to provision of any of the capabilities or services described in 47 C.F.R. § 12.4(a)(4)(i) affecting more than one state, including but not limited to a Covered 911 Service Provider's allocation of such responsibilities to a sub-contractor or other third party.
- (2) Notifications under this section shall be filed with the Commission at least 60 days before the changes described therein take effect.
 - i) Notifications shall state publicly the nature of the proposed changes, the geographic area(s) or jurisdiction(s) affected, the anticipated date of the changes, and any other relevant information.
 - ii) To the extent that notifications contain information that would cause competitive harm or a threat to public safety or national security if disclosed, a Covered 911 Service Provider may request confidential treatment of such information under section 0.459 of the Commission's rules.
 - (3) *Changes initiated by a PSAP or emergency authority.* Changes in 911 network architecture or service initiated by a public safety answering point (PSAP) or state or local emergency authority shall not require a notification to be filed under this section.
 - (4) *Changes subject to public notice under Section 251.* Changes in 911 network architecture or service that require public notice of network changes under 47 C.F.R. § 51.325 shall not require a separate notification under this section.
 - (5) *Emergency changes.* Changes in 911 architecture or services reasonably necessary to mitigate the impacts of a disruption or degradation in 911 service, including temporary re-routes to backup equipment or secondary PSAPs, shall not require a notification to be filed under this section.
- (b) *Discontinuance, reduction, or impairment of existing 911 services.* A Covered 911 Service Provider, as defined in section 12.4(a)(4), seeking to discontinue, reduce, or impair existing 911 services shall file a public notification with the Commission and receive approval from the Commission before undertaking such actions, except as provided in subsections (b)(3) and (b)(4).
 - (1) For purposes of this section, the following actions by a Covered 911 Service Provider constitute a discontinuance, reduction, or impairment of existing 911 services:
 - i) Exit from a line of 911 services previously provided to PSAPs, statewide default answering points, or appropriate local emergency authorities in more than one state;
 - ii) Termination or reduction in technical support or maintenance for 911 network components or customer premises equipment (CPE) to PSAPs, statewide default answering points, or appropriate local emergency authorities in more than one state; or
 - iii) Reduction or impairment of quality-of-service levels for 911 services to PSAPs, statewide default answering points, or appropriate local emergency authorities in more than one state.
 - (2) Applications for discontinuance, reduction, or impairment of existing 911 services under this

section shall be filed with the Commission at least 60 days before the changes described therein are requested to take effect. The Commission shall respond within 60 days by approving the request, approving the request subject to conditions, or denying the request. If the Commission takes no action within 60 days, the request shall be deemed approved.

- i) Applications shall state publicly the nature of the proposed discontinuance, reduction, or impairment, the geographic area(s) or jurisdiction(s) affected, the anticipated date of the changes, and any other relevant information.
 - ii) To the extent that applications contain information that would cause competitive harm or a threat to public safety or national security if disclosed, a Covered 911 Service Provider may request confidential treatment of such information under section 0.459 of the Commission's rules.
- (3) *Changes initiated by a PSAP or emergency authority.* Changes in 911 network architecture or service initiated by a PSAP or state or local emergency authority, including changes that would otherwise constitute a discontinuance, reduction, or impairment of existing 911 services under subsection (b), shall not require Commission approval under this section.
- (4) *Changes subject to Section 214 authorization.* Changes in 911 network architecture or service that require Commission authorization under Section 214 of the Communications Act and associated Commission rules shall not require separate Commission approval under this section.

* * * * *

5. Add section 12.6 to read as follows:

§ 12.6 Reliability and Accountability of New IP-Based 911 Capabilities and Services

- (a) *Certification of capability to provide reliable 911 service.* Entities that propose to provide one or more of the capabilities of a Covered 911 Service Provider, as defined in section 12.4(a)(4), but do not provide such capabilities prior to November 21, 2014, shall certify to the Commission that they:
- (1) Possess the technical and operational capability to provide reliable 911 service;
 - (2) Have conducted a reliability and security risk analysis of any network components, infrastructure and/or databases and software used to support 911 call completion, including automatic location information (ALI), automatic number identification (ANI), location information services (LIS), text-to-911, or the functional equivalent of those capabilities; and
 - (3) Understand and agree to abide by the Commission's annual reliability certification requirements under this Part 12, any applicable outage reporting or PSAP outage notification requirements under 47 C.F.R. § 4.9, and any other Commission rules applicable to the new 911 capabilities that it offers.

* * * * *

6. Add section 12.7 to read as follows:

§ 12.7 Situational Awareness and Coordination Responsibility during Disruptions in 911 Service

- (a) *Designation of 911 Network Operations Center (NOC) Provider.* The Covered 911 Service Provider responsible for transport of 911 calls and associated information to the public safety answering point (PSAP), statewide default answering point, or appropriate local emergency authority in each jurisdiction, pursuant to a contractual relationship with that PSAP, statewide default answering point, or appropriate local emergency authority, shall be the 911 NOC Provider in that jurisdiction.
- (b) *Responsibilities of 911 NOC Provider.* The 911 NOC Provider in each jurisdiction shall monitor the availability of 911 services and coordinate situational awareness and information sharing during disruptions in 911 service. For purposes of this section, disruptions in 911 service include events resulting in a complete loss of 911 service, as well as events that substantially impair service quality or public access to 911 without a complete loss of service, including disruption of automatic location information (ALI), automatic number identification (ANI), location information services (LIS), or any other services that locate callers geographically.
- 1) In the event of such a disruption in 911 service, the 911 NOC Provider shall request information from any other affected Covered 911 Service Provider(s) regarding their situational awareness of the cause and scope of the outage from the origination to the completion of 911 communications, including voice calls, ALI, ANI, LIS, and text-to-911. The 911 NOC Provider shall then communicate to any other affected Covered 911 Service Providers, PSAPs, state emergency management offices, and to the Commission's Operations Center, all information reasonably available to mitigate the effects of the disruption and to restore service.
 - 2) All other Covered 911 Service Providers shall communicate to the 911 NOC Provider all reasonably available information regarding the cause and scope of a disruption in 911 service that occurs on or affects portions of the 911 network that they own, lease, or otherwise operate or control and shall respond promptly to any request for such information by the 911 NOC Provider.

* * * * *

APPENDIX B

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),¹ the Commission has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact of the proposals described in the attached *Policy Statement and Notice of Proposed Rulemaking (Notice)* on small entities. Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments in the *Notice*. The Commission will send a copy of the *Notice*, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).² In addition, the *Notice* and IRFA (or summaries thereof) will be published in the Federal Register.³

A. Need for, and Objectives of, the Proposed Rules

2. The *Notice* seeks comment on governance mechanisms to promote reliable 911 call completion nationwide and improve situational awareness and information sharing among 911 service providers. Specifically, it proposes to (1) amend the Commission's 911 reliability certification rules to cover additional entities and network reliability practices that are vital to call completion; (2) require public notification for major changes in multi-state 911 networks and services, and Commission approval for discontinuance of existing 911 services; (3) require entities seeking to provide new 911 capabilities to certify as to their technical and operational capability to provide reliable service; and (4) designate certain 911 service providers to be primarily responsible for situational awareness and coordination with other service providers in the event of a 911 outage.

3. The *Notice* also affirms core principles guiding the Commission's approach to 911 governance and proposes mechanisms for the Commission, in cooperation with state and local partners, to ensure that the nation's 911 governance structure keeps pace with evolving technology so that all entities providing 911 service capabilities remain accountable for reliable 911 call completion and accurate situational awareness. As discussed in the *Notice*, recent outage trends have revealed new reliability challenges due to geographic consolidation of network infrastructure and an increasing reliance on software-based network components to process and route 911 calls on a regional or national scale. Furthermore, an increasing number of 911 service providers subcontract with third party vendors for call-routing and other technical capabilities that are essential to call completion. As a result, 911 call centers potentially face real-time communication problems in trying to mitigate 911 service problems with 911 service providers and subcontractors. The Commission has a responsibility to promote reliable emergency communications and prevent avoidable failures.

4. The *Notice* builds upon the *911 Reliability Order* adopted by the Commission in 2013 following the 2012 derecho storm,⁴ and sets forth principals to guide the Commission's 911 governance efforts in light of technology transitions and changing outage trends. In particular, the *Policy Statement* affirms the Commission's policy of working with state and local partners to ensure reliable 911 call completion as technology transitions consolidate network infrastructure and change the way 911 services are delivered to PSAPs in multiple states. Further, the Commission stresses that service provider changes

¹ See 5 U.S.C. § 603. The RFA, see 5 U.S.C. § 601 – 612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

² See 5 U.S.C. § 603(a).

³ See 5 U.S.C. § 603(a).

⁴ See Reliability and Continuity of Communications Networks, Including Broadband Technologies, PS Docket Nos. 13-75, 11-60, *Report and Order*, 28 FCC Rcd 17476 (2013) (*911 Reliability Order*).

to 911 services must be transparent and coordinated with the Commission and the appropriate state and local authorities.

B. Legal Basis

5. The legal basis for any action that may be taken pursuant to this Notice of Proposed Rulemaking is contained in Sections 1, 4(i), 4(j), 4(o), 5(c), 201(b), 214(d), 218, 219, 251(e), 301, 303(g), 303(j), 303(r), 332, 403, 615, 615a, 615c, 621(b)(3), and 621(d) of the Communications Act of 1934, 47 U.S.C. §§ 151, 154(i), 154(j), 154(o), 155(c), 201(b), 214(d), 218, 219, 251(e), 301, 303(b), 303(g), 303(j), 303(r), 332, 403, 615, 615a, 615c, 621(b)(3), and 621(d).

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Would Apply

6. The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules.⁵ The RFA generally defines the term “small entity” as having the same meaning as the terms “small business,” “small organization,” and “small governmental jurisdiction.”⁶ In addition, the term “small business” has the same meaning as the term “small business concern” under the Small Business Act.⁷ A small business concern is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the Small Business Administration (SBA).⁸

7. *Small Businesses, Small Organizations, and Small Governmental Jurisdictions.* Our action may, over time, affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three comprehensive, statutory small entity size standards.⁹ First, nationwide, there are a total of approximately 27.5 million small businesses, according to the SBA.¹⁰ In addition, a “small organization” is generally “any not-for-profit enterprise which is independently owned and operated and is not dominant in its field.”¹¹ Nationwide, as of 2007, there were approximately 1,621,315 small organizations.¹² Finally, the term “small governmental jurisdiction” is defined generally as “governments of cities, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand.”¹³ Census Bureau data for 2011 indicate that there were 89,476 local governmental jurisdictions in the United States.¹⁴ We estimate that, of this total, as many as 88,506

⁵ 5 U.S.C. §§ 603(b)(3), 604(a)(3).

⁶ 5 U.S.C. § 601(6).

⁷ 5 U.S.C. § 601(3) (incorporating by reference the definition of “small business concern” in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies “unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such terms which are appropriate to the activities of the agency and publishes such definitions(s) in the Federal Register.”

⁸ 15 U.S.C. § 632.

⁹ See 5 U.S.C. §§ 601(3)–(6).

¹⁰ Figure is from 2011. See SBA, Office of Advocacy, available at http://www.sba.gov/sites/default/files/FAQ_March_2014_0.pdf (last viewed Oct. 27, 2014).

¹¹ 5 U.S.C. § 601(4).

¹² INDEPENDENT SECTOR, THE NEW NONPROFIT ALMANAC & DESK REFERENCE (2010).

¹³ 5 U.S.C. § 601(5).

¹⁴ U.S. CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES: 2011, Table 427 (2007).

entities may qualify as “small governmental jurisdictions.”¹⁵ Thus, we estimate that most governmental jurisdictions are small.

8. The *Notice* seeks comment on the class of entities to which the proposals would apply. In the *Derecho Report* and the *911 Reliability Order* the Commission defined “covered 911 service providers,” as those that provide specified 911 capabilities, or the functional equivalent, “directly to a PSAP.” The *Notice* asks whether the Commission should expand the “covered 911 service providers” definition to also include all entities that provide 911, E911, or NG911 capabilities, such as call routing, automatic location information (ALI), automatic number identification (ANI), location information servers (LIS), text-to-911, or the functional equivalent of those capabilities, regardless of whether they provide such capabilities under a direct contractual relationship with a PSAP or emergency authority. Depending on how 911 calls are routed and processed in different network architectures, the proposed definition could apply to originating service providers (OSPs) such as wireless carriers and interconnected VoIP providers, incumbent local exchange carriers (ILECs), 911 system service providers (SSPs) that provide 911 services such as call routing and location information to PSAPs, and vendors and subcontractors of such entities to the extent that they provide covered 911 capabilities.

9. The *Notice* seeks comment on which 911 service providers should be subject to additional 911 network change notification requirements, including publicly reporting major changes in their respective facilities and networks that affect PSAPs in multiple states. To the extent that changes in 911 service amount to a discontinuance, reduction, or impairment of existing services, the *Notice* proposes to require Commission approval to the extent that authorization is not already required under Section 214 of the Communications Act. The *Notice* also seeks comment on whether to require 911 entities that propose to offer new services that affect 911 call completion to certify with the Commission baseline assurances of their technical and operational qualifications to provide reliable 911 service, as well as comment on which 911 entities should be subject to this certification.

10. To facilitate situational awareness and coordination, the *Notice* seeks comment on the establishment of a class “911 Network Operations Center (911 NOC) providers,” which would assume primary responsibility for situational awareness and information sharing during disruptions in 911 service. The *Notice* proposes that the 911 NOC provide role for each jurisdiction should be assigned to the entity responsible for transport of 911 traffic to the PSAP or PSAPs serving that jurisdiction – typically the local ILEC in legacy network architectures. However, as we transition into IP-based NG911 networks, other entities such as SSPs and emergency services Internet Protocol network (ESINet) providers may receive 911 traffic from an OSP and then direct traffic to the PSAP. The *Notice* seeks comment on whether ILECs, ESINet providers or other 911 call transport entities should be the 911 NOC providers under this proposal.

1. Communications Service Entities

11. *Incumbent Local Exchange Carriers (Incumbent LECs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. The appropriate size standard under SBA rules is for the category Wired Telecommunications Carriers.

¹⁵ The 2007 U.S Census data for small governmental organizations are not presented based on the size of the population in each such organization. There were 89,476 small governmental organizations in 2007. If we assume that county, municipal, township and school district organizations are more likely than larger governmental organizations to have populations of 50,000 or less, the total of these organizations is 52,125. If we make the same assumption about special districts, and also assume that special districts are different from county, municipal, township, and school districts, in 2007 there were 37,381 special districts. Therefore, of the 89,476 small governmental organizations documented in 2007, as many as 89,506 may be considered small under the applicable standard. This data may overestimate the number of such organizations that has a population of 50,000 or less. U.S. CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES 2011, Tables 427, 426 (Data cited therein are from 2007).

Under that size standard, such a business is small if it has 1,500 or fewer employees.¹⁶ Census Bureau data for 2007, which now supersede data from the 2002 Census, show that there were 3,188 firms in this category that operated for the entire year. Of this total, 3,144 had employment of 999 or fewer, and 44 firms had had employment of 1000 or more. According to Commission data, 1,307 carriers reported that they were incumbent local exchange service providers.¹⁷ Of these 1,307 carriers, an estimated 1,006 have 1,500 or fewer employees and 301 have more than 1,500 employees.¹⁸ Consequently, the Commission estimates that most providers of local exchange service are small entities that may be affected by the rules and policies proposed in the *Notice*. Thus under this category and the associated small business size standard, the majority of these incumbent local exchange service providers can be considered small.¹⁹

12. *A Competitive Local Exchange Carriers (Competitive LECs), Competitive Access Providers (CAPs), Shared-Tenant Service Providers, and Other Local Service Providers.* Neither the Commission nor the SBA has developed a small business size standard specifically for these service providers. The appropriate size standard under SBA rules is for the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.²⁰ Census Bureau data for 2007, which now supersede data from the 2002 Census, show that there were 3,188 firms in this category that operated for the entire year. Of this total, 3,144 had employment of 999 or fewer, and 44 firms had had employment of 1,000 employees or more. Thus under this category and the associated small business size standard, the majority of these Competitive LECs, CAPs, Shared-Tenant Service Providers, and Other Local Service Providers can be considered small entities.²¹ According to Commission data, 1,442 carriers reported that they were engaged in the provision of either competitive local exchange services or competitive access provider services.²² Of these 1,442 carriers, an estimated 1,256 have 1,500 or fewer employees and 186 have more than 1,500 employees.²³ In addition, 17 carriers have reported that they are Shared-Tenant Service Providers, and all 17 are estimated to have 1,500 or fewer employees.²⁴ In addition, 72 carriers have reported that they are Other Local Service Providers.²⁵ Of the 72, seventy have 1,500 or fewer employees and two have more than 1,500 employees.²⁶ Consequently, the Commission estimates that most providers of competitive local exchange service, competitive access providers, Shared-Tenant Service Providers, and Other Local Service Providers are small entities that may be affected by rules proposed in the *Notice*.

13. *Wireless Telecommunications Carriers (except satellite).* This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular phone services, paging services, wireless Internet access,

¹⁶ 13 C.F.R. § 121.201, NAICS code 517110.

¹⁷ See *Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

¹⁸ See *id.*

¹⁹ See http://factfinder.census.gov/servlet/IBQTable?_bm=y&-fds_name=EC0700A1&-geo_id=&-skip=600&-ds_name=EC0751SSSZ5&-lang=en.

²⁰ 13 C.F.R. § 121.201, NAICS code 517110.

²¹ See http://factfinder.census.gov/servlet/IBQTable?_bm=y&-fds_name=EC0700A1&-geo_id=&-skip=600&-ds_name=EC0751SSSZ5&-lang=en.

²² See *Trends in Telephone Service* at Table 5.3.

²³ See *id.*

²⁴ See *id.*

²⁵ See *id.*

²⁶ See *id.*

and wireless video services.²⁷ The appropriate size standard under SBA rules is for the category Wireless Telecommunications Carriers. The size standard for that category is that a business is small if it has 1,500 or fewer employees.²⁸ For this category, census data for 2007 show that there were 11,163 establishments that operated for the entire year.²⁹ Of this total, 10,791 establishments had employment of 999 or fewer employees and 372 had employment of 1000 employees or more.³⁰ Thus under this category and the associated small business size standard, the Commission estimates that the majority of wireless telecommunications carriers (except satellite) are small entities that may be affected by rules proposed in the Notice.³¹

14. *Wireless Service Providers.* The SBA has developed a small business size standard for wireless firms within the two broad economic census categories of “Paging” and “Cellular and Other Wireless Telecommunications.” Under both categories, the SBA deems a wireless business to be small if it has 1,500 or fewer employees. For the census category of Paging, Census Bureau data for 2002 show that there were 807 firms in this category that operated for the entire year. Of this total, 804 firms had employment of 999 or fewer employees, and three firms had employment of 1,000 employees or more. Thus, under this category and associated small business size standard, the majority of firms can be considered small. For the census category of Cellular and Other Wireless Telecommunications, Census Bureau data for 2002 show that there were 1,397 firms in this category that operated for the entire year. Of this total, 1,378 firms had employment of 999 or fewer employees, and 19 firms had employment of 1,000 employees or more. Thus, under this second category and size standard, the majority of firms can, again, be considered small.

15. *All Other Telecommunications Providers.* To the extent that entities such as SSPs and interconnected VoIP providers are subject to proposals in the *Notice* but are not “Wired Telecommunication Carriers,” “Wireless Telecommunication Carriers,” or “Cellular and Other Wireless Telecommunications” under the categories listed above, the closest U.S. Census category appears to be “All Other Telecommunications.” All Other Telecommunications is defined as follows: “This U.S. industry comprises establishments primarily engaged in providing specialized telecommunications services, such as . . . Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections.”³² In analyzing whether a substantial number of small entities would be affected by the requirements proposed in the *Notice*, the Commission notes that the SBA has developed a small business size standard for All Other Telecommunications, which consists of all such firms with gross annual receipts of \$30 million or less.³³ For this category, census data for 2007 show that there

²⁷ U.S. Census Bureau, North American Industry Classification System, Definition of “Wireless Telecommunications Carriers (except Satellite),” NAICS code 517210, available at <http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517210&search=2007%20NAICS%20Search> (last viewed Jan. 31, 2013).

²⁸ See *id.* See also 13 C.F.R. § 121.201, NAICS code 517210.

²⁹ U.S. Census Bureau, Subject Series: Information, Table 5, “Establishment and Firm Size: Employment Size of Firms for the United States: 2007 NAICS Code 517210” (issued Nov. 2010), available at http://factfinder2.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2007_US_51SSSZ2&prodType=table (last viewed Jan. 31, 2014).

³⁰ *Id.* Available census data do not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is for firms with “100 employees or more.”

³¹ *Id.*

³² U.S. Census Bureau, North American Industry Classification System, Definition of “All Other Telecommunications,” NAICS code 517919, available at <http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517919&search=2007%20NAICS%20Search> (last viewed Nov. 18, 2014).

³³ See 13 C.F.R. § 121.201, NAICS code 517919 (2012).

were 2,639 establishments that operated for the entire year.³⁴ Of those establishments, a total of 1,912 had gross annual receipts between \$100,000 and \$1 million; 487 had gross annual receipts between \$1 million and \$25 million; and 240 had gross annual receipts over \$25 million.³⁵ Thus, a majority of All Other Telecommunications firms potentially affected by the proposals in the *Notice* can be considered small.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

16. As noted above, the *Notice* proposes to (1) amend the Commission's 911 reliability certification rules to cover additional entities and network reliability practices that are vital to call completion; (2) require public notification for major changes in multi-state 911 networks and services, and Commission approval for discontinuance of existing 911 services; (3) require entities seeking to provide new 911 capabilities to certify as to their technical and operational capability to provide reliable service; and (4) designate certain 911 service providers to be primarily responsible for situational awareness and coordination with other service providers in the event of a 911 outage.

17. The *Notice* proposes that a covered 911 service provider take reasonable measures to provide reliable service and complete an annual certification indicating whether it has implemented specified best practices or reasonable alternative measures. Covered 911 service providers' "reasonable measures" obligation would include—but would not be limited to—existing areas of circuit diversity, central-office backup power, and diverse network monitoring. Further, covered 911 service providers' certifications to the Commission would indicate whether IP-based 911 architecture is geographically distributed, load-balanced, and capable of automatic reroutes to backup equipment in the event of a hardware, network, software or database failure. The networking monitoring section of the certification would also include current requirements for physical diversity of monitoring facilities, but also the proper prioritization of critical network alarms. Further, the *Notice* proposes that 911 entities have a duty to take reasonable measures to communicate with other 911 entities during disruptions in 911 service. Providers would be required to certify whether they have an outage notification process in place to notify PSAPs of disruptions in 911 service within time frames specified in Part 4 of the Commission rules.

18. These proposals build upon the existing 911 reliability certification process for covered 911 service providers that the Commission established in 2013.³⁶ Under this process, a corporate officer with supervisory and budgetary authority over network operations in all relevant service areas must file an annual attestation with the Commission describing the entity's implementation of specified best practices, or if it is not feasible to implement those best practices, a description of reasonable alternative measures designed to mitigate the risk of failure. The option of certifying alternative measures is designed to provide flexibility to small entities operating in diverse service areas, which may have unique ways of addressing network reliability challenges. Because many covered 911 service providers have indicated they already conduct activities that form the basis for this certification in the normal course of business, the Commission expects the additional burden of filing certifications to be minimal. Certifications will be submitted through a simple online form, which is designed to allow small entities to input certification information and upload an attestation from a corporate officer without the need for any specialized personnel. In some cases, however, covered 911 service providers may choose to hire consultants or engineers to conduct technical aspects of the certification, or an attorney to review certification information for compliance with applicable rules. However, the Commission expects that

³⁴ U.S. Census Bureau, Information: Subject Series - Establishment and Firm Size: Receipts Size of Firms for the United States: 2007 NAICS Code 517919, *available at* http://factfinder2.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2007_US_51SSSZ4&prodType=table (last viewed Nov. 18, 2014).

³⁵ *Id.*

³⁶ *See 911 Reliability Order*, 28 FCC Red 17476; 47 C.F.R. § 12.4.

most covered 911 service providers, including small entities, will be able to complete and submit the annual certification using only in-house personnel.

19. The *Notice* proposes to require notification to the Commission and the public of major changes in any 911 service provider's network architecture or scope of 911 services that are not otherwise covered by existing network change notification requirements. The *Notice* seeks comment on the specific changes that would be subject to notification requirements but proposes generally that changes affecting 911 service to PSAPs in multiple states would be considered "major" and subject to public notification. The proposed notifications would be filed with the Commission in a process similar to the existing network change notifications required from incumbent LECs under Section 251 of the Communications Act.³⁷ These are typically relatively short filings describing the nature of the planned changes and location(s) affected.³⁸ Some companies may wish to have an attorney review such notifications for compliance purposes, but the proposal does not require such a review.

20. For incumbent 911 service providers that seek to discontinue, reduce or impair existing 911 service in a way that does not trigger already existing authorization requirements under Section 214 of the Communications Act, the *Notice* proposes to require prior Commission approval. The *Notice* seeks comment on which actions by an incumbent 911 service provider would be considered a discontinuance, reduction or impairment of service. However, this proposal would not include changes requested by a PSAP or the responsible state or local emergency authority that might otherwise constitute a discontinuance, reduction or impairment of service. Commission approval under this proposal would require the applicant to file a request to discontinue, reduce, or impair 911 services stating the nature of the changes, the location(s) affected, and the anticipated date of the changes. If the Commission does not act on such a request within 60 days, the request will be deemed approved. As noted above, certain applicants may wish to hire engineers, consultants, or attorneys to review applications for discontinuance or technical portions thereof, but there is no such requirement in the proposed rule.

21. The *Notice* also proposes to require covered 911 service providers that seek to offer new services that affect 911 call completion to certify to the Commission that they have the technical and operational capability to provide reliable 911 service. To the extent that the new services rely on IP-based networks, associated infrastructure such as servers and data centers, and/or associated software applications, the *Notice* proposes that covered 911 service providers certify that they have conducted a reliability and security risk analysis of the network components, infrastructure, and/or software that they will use to support 911 call completion. This proposal would not require Commission approval of new entrants or delay the introduction of new 911 technologies. It would, however, require entities that seek to provide new critical links in 911 call completion to publicly acknowledge their responsibilities and certify their preparedness to implement relevant best practices and comply with existing Commission rules applicable to the 911 capabilities they provide. The Commission does not anticipate the need for any specialized personnel to provide such a certification.

22. To improve situational awareness during 911 outages, the *Notice* proposes to establish a class of "911 Network Operations Center (911 NOC) providers," which would assume primary responsibility for monitoring their networks to detect disruptions or degradations in 911 service, and for affirmatively communicating relevant information, as appropriate, to other affected 911 entities, including OSPs, SSPs, vendors, PSAPs, state emergency management offices, and the Commission's Operations Center. The role of the 911 NOC provider would be assigned to the entity responsible for transport of 911 traffic to the PSAP(s) in each jurisdiction. 911 NOC providers would receive information from, and coordinate with other covered 911 service providers to collect and distribute information regarding the impact of outages on all affected portions of the network from call origination to completion. The *Notice*

³⁷ See 47 C.F.R. § 51.325(a).

³⁸ See Section 251 Wireline Network Changes, <http://www.fcc.gov/encyclopedia/section-251-wireline-network-changes> (displaying recent notifications filed by ILECs pursuant to 47 C.F.R. §§ 51.325 – 51.335).

seeks comment on other responsibilities of the 911 NOC provider, as well as the responsibilities of other covered 911 service providers to share information with the 911 NOC provider. The Commission anticipates that most or all of these information-sharing activities would be performed by in-house personnel who already are employed to monitor and maintain covered 911 service providers' networks. In any event, the *Notice* proposes that 911 NOC providers would not be legally responsible for outages attributable to failures of network components outside their control, or for remediating or repairing such failures.

E. Steps Taken to Minimize Significant Economic Impact on Small Entities, and Significant Alternatives Considered

23. The RFA requires an agency to describe any significant, specifically small business alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): “(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for small entities; (3) the use of performance, rather than design, standards; and (4) and exemption from coverage of the rule, or any part thereof, for small entities.”³⁹

24. The *Notice* seeks to update and enhance the Commission's current 911 reliability certification rules, which complement its general approach of encouraging communications providers to voluntarily implement best practices and measuring compliance through certification requirements and outage reporting. Thus, small entities with limited resources would continue to enjoy many of the benefits of the current regime, including a general focus on network performance and reliability rather than specific design requirements. The option to certify reasonable alternative measures in lieu of specified certification requirements also provides flexibility to small entities, and the online system for submission of certification information is designed for ease of use by all communications providers without the need for specialized personnel. Public notifications and certifications proposed in the *Notice* would follow similar submission processes and would not mandate any specific standards for 911 network architecture. The Commission has traditionally considered this approach a more flexible and less costly alternative to more comprehensive regulation, and the *Notice* would preserve those advantages in large part.

25. Furthermore, the proposals in the *Notice* apply primarily to service providers that offer 911 services on a multi-state scale to PSAPs in multiple jurisdictions. For example, IP-based 911 call routing capabilities are typically concentrated in a small number of servers and databases that may serve PSAPs across the country. Our proposals with respect to public notification and Commission approval of major changes in 911 service or discontinuance of 911 service also would apply only to providers serving PSAPs in multiple states. Thus, while there is no explicit exemption proposed for small entities, many of the rules by their nature will tend to apply only to larger communications providers that operate major, multi-state 911 networks.

26. To the extent that the *Notice* would impose new obligations on small entities, we seek comment on alternatives including (1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for small entities; (3) the use of performance, rather than design, standards; and (4) an exemption from coverage of the rule, or any part thereof, for small entities.⁴⁰ Which of the proposed approaches do small entities find particularly difficult or costly to comply with, and how could those difficulties be addressed through modifications or exemptions? What would be the effect on public safety of exemptions from 911 service requirements, regardless of cost?

³⁹ 5 U.S.C. §§ 603(c)(1)-(c)(4).

⁴⁰ *Id.*

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

27. None.

**STATEMENT OF
CHAIRMAN TOM WHEELER**

Re: *911 Governance and Accountability*, PS Docket No. 14-193; *Improving 911 Reliability*, PS Docket No. 13-75

Technology transitions are changing the way calls to 911 are processed and completed across America. Tremendous benefits can be realized by the transition of public safety communications to IP-based networks. For example, IP-based Next Generation 911 networks will enable call centers to receive a greater range of information – such as text, video, and data from vehicle crash sensors – to better support first responders in an emergency.

We must encourage these new capabilities through 911 governance policies that support and reward innovation while ensuring that sufficient protections are in place so that Americans can be sure 911 will work when they need it to work.

The introduction of new technologies forces us to change the way we think about these services, and introduces new vulnerabilities that we cannot ignore.

For example, the process of routing and completing a single 911 call now often involves multiple companies, operating different parts of the call chain, located in different states, all of whom are potentially thousands of miles away from where the actual call is placed. That means a single failure in one location can leave millions people without 911 service across multiple states, indeed across the nation.

With 911 capabilities that were previously provided by a single company divided among several companies spread out across the country, we at the Federal level must work hand in glove with our state and local colleagues to preserve accountability for reliable service at each link in the call-completion chain.

Additionally, we are all used to thinking about 911 outages as result of natural disasters – tornados, hurricanes, derechos – with localized impact. However, we have seen a spike in so-called “sunny day” outages caused by preventable software glitches or databases failures – not “acts of God.”

As the Public Safety Bureau reported to the Commission in October, a “sunny day” outage this past April left more than 11 million consumers in 7 states without 911 service for up to 6 hours. Some 6,600 calls for help to 911 were not completed during that time. This is unacceptable.

States and localities play an essential role in 911 governance, and their continued oversight is vital to ensuring that 911 service remains effective and reliable in every community. The item we adopt today proposes a framework for 911 governance that ensures state and local partners continue to be empowered to fulfill this important oversight responsibility within their jurisdictions. Together with state and local partners, we can – and will – ensure that there are no gaps in oversight, through the technology transition and into the future.

Specifically, the NPRM proposes a 911 governance structure designed to ensure that technology transitions are managed in a way that maximizes the availability, reliability, and resiliency of 911 networks, as well as the accountability of all participants in the 911-call completion process. These collaborative, technology-neutral proposals underscore the Commission’s commitment to working with state and local partners to protect the enduring values that consumers have rightly come to expect from their communications providers.

As the world evolves to next generation 911 systems, the FCC has a responsibility to ensure Americans are confident that the service they rely on to reach first responders is reliable, providers are accountable and 911 is always accessible in their time of need.

**STATEMENT OF
COMMISSIONER MIGNON L. CLYBURN**

Re: *911 Governance and Accountability*, PS Docket No. 14-193; *Improving 911 Reliability*, PS Docket No. 13-75.

Over the years, the Commission has adopted a number of items to promote the deployment of Next Generation or NG 9-1-1 networks. Designed appropriately, carriers will be able to provide state of the art emergency communications services using the most advanced IP technologies, allowing consumers to give first responders additional information, in more ways, during an emergency.

But last month's report on the 2014 multi-state sunny day outages was a reminder that any transition without the proper safeguards -- no matter how promising the technology -- could bring undesirable outcomes. In one case, a software coding error prevented more than 6,600 emergency calls from reaching 81 PSAPs in seven states (including my home state of South Carolina) and an inadequate alarm management brought about a significant delay in the identification of the software fault and full restoration of emergency service.

IP technologies can help carriers consolidate 9-1-1 infrastructure, across several states develop economies of scale, and consequently, dramatically lower the costs of delivering these critical services, resulting in significant public interest benefits, for which we should support. But no amount of efficiency of scale or scope can come at the expense of accountability, redundancy, and coordination -- all of which are fundamental to running any viable communications business. I focused on a few words at the beginning of paragraph seven of this Policy Statement and NPRM, which sum it up for me: "Our goal of proactive, measured accountability for reliable 9-1-1 completion" must identify which part of the 9-1-1 system has failed, which provider is responsible for those repairs, and who is responsible for providing timely and comprehensive information to PSAPs and the public. So, I commend Chairman Wheeler for circulating an NPRM that sends two clear messages. First, any new elements of 9-1-1 architecture or service should have the necessary safeguards, along with the appropriate governance mechanisms, to maximize reliability and protect public safety. And second, significant changes in service should be coordinated in a transparent manner with the Commission and with state and local authorities. Today, we propose common sense rules to implement those principles, which include changing the Commission's reliability certification rules to cover additional entities, requiring public notification for major changes in multi-state networks and designating certain service providers to be responsible for primary coordination in the event of an outage.

The days of 9-1-1 services solely provided by incumbent carriers seem to be far behind us, but the responsibility for the integrity of these critical networks remains the same. I wish to thank Admiral David Simpson and Eric Schmidt for their presentations. It's good to see my former colleague, Commissioner Phil Jones, here and his decision to travel from the state of Washington to be with us today underscores the importance of this action today.

Also, I want to recognize, David Furth, Erika Olsen, Nikki McGinnis, Clete Johnson, Tim May, Jeff Goldthorp, Lauren Kravetz, John Healy, Jerry Stanshine and one of the new Honors attorneys at the FCC, Brenda Villanueva, for their contributions on an item that recognizes precisely where the buck stops.

**STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL**

Re: *911 Governance and Accountability*, PS Docket No. 14-193; *Improving 911 Reliability*, PS Docket No. 13-75.

You may only make one 911 call in your life, but as the old saw goes, it will be the most important call you ever make. No matter the time and no matter the technology, you need to know that your call will be answered and that first responders can find you.

The challenge for the future of 911 is one that is common to other areas of communications. The ways we connect are changing at a blistering pace. Our networks are both more complex and more diverse than ever before. In the face of all this change, we need to double down and ensure that emergency communications systems are updated, secure, resilient, and reliable.

At the Commission, we have been on a multi-year course to modernize our emergency communications policies. After all, it was not that long ago that emergency calls to 911 came only from landlines. But over time, we expanded this service to mobile phones. Later, we made 911 an essential feature of interconnected VoIP service. Just a few months ago, we brought texting into the 911 fold.

We need to continue on this course. That means we must always be on guard for new vulnerabilities and gaps in the safety of our 911 systems.

We saw one such gap earlier this year when 81 911 call centers in seven states lost service for as long as six hours. As a result, thousands of people who called 911 were unable to receive the help they needed. Instead, when they reached out in crisis, they got silence at the end of the line.

So we studied. We worked with carriers, public safety officials, and our state counterparts. We learned that this multistate outage was caused by a coding error—a software glitch that stopped calls from being routed through the network to affected 911 call centers. But it is not enough to know what went wrong. We need to do something about it.

Today we propose solutions to close this gap. We propose to take our certification requirements and apply them to all entities providing essential 911 capabilities. We propose reporting requirements for outages. We also encourage states and localities to work with us as networks change and our emergency communications systems require upgrades. These ideas are commonsense—and I support them.

But while we work to close this gap, we need to be mindful of others. Today, more than 70 percent of 911 calls are made from wireless phones. That is more than 400,000 calls across the country every day. And this number is only going to grow. Because for roughly two in five households, their wireless phone is their only phone.

Despite this nationwide change in calling practices, our rules that provide first responders with information about where they are when we call 911 are stranded in calling practices of the last century. They help first responders find you when you call from a landline phone. They assist first responders with locating you when you call from a wireless phone outdoors. But if you call from a wireless phone indoors, no location accuracy standards apply.

This too is a gap. Like the one we address today and the others we have addressed before—it requires our attention. Because no matter how communications changes, when a crisis occurs, you need your call to go through and you need first responders to find you.

**DISSENTING STATEMENT OF
COMMISSIONER AJIT PAI**

Re: *911 Governance and Accountability*, PS Docket No. 14-193; *Improving 911 Reliability*, PS Docket No. 13-75.

At last month's Commission meeting, we heard about a 911 outage that affected over 11 million people across seven different states.¹ As I said then, such outages are unacceptable.² Providers of 911 services have a special responsibility to ensure that they abide by best practices, including maintaining redundant and reliable networks. And the FCC has an important role to play. There are steps we can and should take to help improve 911 reliability, facilitate the transition to NG911, and guard against multi-state outages. In fact, the law requires us to support the lead role state and local public safety officials play in overseeing the provision of 911 service.

Unfortunately, today's Notice of Proposed Rulemaking heads in an entirely different direction. It proposes to supplant the efforts of our nation's first responders with what the NPRM says is a new and "comprehensive" "national governance structure"—one that would apply federal regulation to every aspect of 911 service.³ Replacing state and local governance with Washington-knows-best bureaucracy will leave 911 systems less nimble and responsive to the needs of local communities. It will deter the introduction of innovative and reliable 911 services. It will impose unnecessary costs on state and local 911 officials. And it will do all this in the glaring absence of legal authority. Because I cannot support this proposed federal takeover of the 911 system, I dissent.

Turning to the specifics, the NPRM's proposals will deter the introduction of reliable and innovative 911 solutions that public safety officials want and need. How so? Well, any 911 provider that wants to enter the market would first need to certify its qualifications to the FCC, including (the NPRM suggests) obtaining and submitting third-party certifications. The information required could cover such wide-ranging areas as supply chain risk management and analysis of the software the provider would use.

Think about that for a second. A local PSAP that wants to take advantage of a new, innovative 911 offering could very well hear from the FCC: Sorry, you can't receive that service. But how is this agency better positioned than local 911 officials to determine what offerings are appropriate to meet their communities' particular needs? How many 911 providers will simply decide not to offer an innovative, new capability because of the FCC's all-encompassing process? Micromanagement from Washington is neither appropriate nor effective, even if we were equipped to carry it out.

Yet the item goes still further. If for any reason a covered provider wants to reduce or stop offering a 911 capability, it would first have to get the FCC's permission. For example, if you launch a smartphone app that has 911 functionality, the FCC would decide when, if, and on what terms you can limit or stop offering the capability. It doesn't matter why you want to do so. This federal chokepoint on exiting a market will deter providers from entering it in the first place.

Additionally, the proposed rules will hamstring 911 service providers and prevent them from quickly making necessary improvements. Before making any number of changes—including how they route 911 calls or assign responsibility for technical support—they would need to file a public notice with

¹ FCC Public Safety & Homeland Security Bureau, *April 2014 Multistate 911 Outage: Cause and Impact*, PS Docket No. 14-72, PSHSB Case File Nos. 14-CCR-0001-0007 (Oct. 2014), <http://go.usa.gov/sztw>.

² Remarks of Commissioner Ajit Pai on the Presentation on the April 2014 Multistate 911 Outage Report (Oct. 17, 2014), <http://go.usa.gov/sfuC>.

³ *See, e.g., NPRM* at para. 36.

the FCC, provide detailed information about the proposed change, and then wait at least 60 days before moving forward. Imposing mandatory, across-the-board waiting periods will not produce an agile, responsive 911 system.

We ought not neglect or understate the Rubicon the FCC aims to cross with this action. The Commission may soon dismantle the longstanding governance structure of the 911 system, in which state and local authorities take a leading role. Many in the public safety community have repeatedly warned the federal government against doing this. Just last week, local 911 authorities told the FCC that “[l]ocal and state authorities[,] rather than the Commission, should take the lead in 9-1-1 governance and oversight, and drive 9-1-1 policy and regulation[.]”⁴ They stated that “[g]overnance and oversight should be at the state level, where it can be most responsive to local constituents’ and public safety agency needs and considerations.”⁵ Others, like the National Emergency Number Association, have stated that “there is a clear consensus that states will play a central role in the deployment of NG9-1-1, and that the Federal government’s chief role will be facilitation, rather than control.”⁶

The Commission itself agrees—at least, it used to. Just last year, when the FCC provided Congress with recommendations for an NG911 statutory framework, it didn’t even ask for authority to create the federal regime we propose today. Instead, it noted the consensus view that “state and local authorities should retain their primary role in the management and development of NG911.” It was unambiguous in stating that state and local “oversight authority . . . should not be supplanted by the federal government.”⁷ It told Congress that the federal government should remain “focused on supporting and coordinating state and local transition efforts.” And it “recommend[ed] that Congress recognize the importance of state 911 boards and state-level governance entities in the cost-effective and efficient implementation of emergency services.”⁸

Retaining the primacy of state and local authorities is not simply a matter of choice. It is the law. State and local governments take the lead oversight role because that is what the law requires. Congress created both a clear and limited role for the Commission. The Communications Act affords us the power to “encourage and support efforts by States”⁹ and to “work cooperatively . . . to develop best practices[.]”¹⁰ Our role is a supplementary one—and no more.

There simply is no law that gives the FCC the authority to create the comprehensive federal 911 regime we propose today. In straining to reach a contrary conclusion, the NPRM goes so far as to rely on a statutory provision that expressly states that it does not “authorize . . . the Commission to impose obligations . . . on any person.”¹¹ I realize objections about legal authority exasperate those who just want to “do something,” but this borders on the absurd. And batting aside these objections won’t do us any favors if and when our decisions are challenged in court.

⁴ Letter from Joseph P. Benkert, Counsel to Boulder Regional Emergency Telephone Service Authority (BRETSA), to Marlene H. Dortch, Secretary, FCC at 2 (Nov. 14, 2014), <http://go.usa.gov/sF25>.

⁵ Letter from Joseph P. Benkert, Counsel to Boulder Regional Emergency Telephone Service Authority (BRETSA), to Marlene H. Dortch, Secretary, FCC at 6 (Nov. 14, 2014), <http://go.usa.gov/sF2V>.

⁶ Reply Comments of NENA at 2, PS Docket No. 12-333 (Jan. 14, 2013), <http://go.usa.gov/sF2H>.

⁷ FCC, Legal and Regulatory Framework for Next Generation 911 Services, Report to Congress and Recommendations at 4.1.1 (2013), <http://go.usa.gov/sFTG>.

⁸ *Id.* at 4.1.1.2.2 and 4.1.1.2.

⁹ 47 U.S.C. § 615.

¹⁰ 47 U.S.C. § 615a-1.

¹¹ *See NPRM* at paras. 38, 76, 87 (relying on 47 U.S.C. § 615).

Yet here we are. Without any legal backing, we are proposing to regulate any entity that operates in the 911 space. Entry and exit requirements will be determined by the FCC, and every component of a 911 provider's offering will be subject to agency review. That doesn't leave much room for local and state authorities to play a "lead" oversight role—except, of course, if we are telling them to lead from behind.

Obviously, when there are breakdowns in the 911 system, the FCC should not just sit around twiddling its thumbs. We do have a critical role to play, even if it's a limited one. There is more we can and should do to support and encourage state and local responses to 911 outages. There is more we can and should do to help develop best practices that ensure the reliability of the 911 system. And there is more we can and should do to help coordinate state and regional responses to 911 failures, particularly those that impact consumers across state lines. That is why, for example, I suggested that this item seek comment on how the FCC can facilitate the ability of state or regional bodies to coordinate on 911 outage and governance issues that transcend state boundaries. And I am glad that at least some of the original NPRM's more intrusive entry regulation proposals are no longer on the table.

But in the end, our differences on this item proved too great to bridge. I cannot support proposals that we have no legal authority to adopt, that will ossify the 911 system, that will impede innovative and reliable solutions, and that will make the FCC an ill-suited but all-powerful gatekeeper for providers seeking to enter or exit the market. And I will not support an effort to supplant those public safety officials who are on the front lines in communities across our nation every single day. For all of these reasons, I respectfully dissent

**DISSENTING STATEMENT OF
COMMISSIONER MICHAEL O'RIELLY**

Re: *911 Governance and Accountability*, PS Docket No. 14-193; *Improving 911 Reliability*, PS Docket No. 13-75

Less than a year after the Commission adopted the 911 reliability order, and before carriers have even filed their first certifications, we are seeking comment on further expanding the requirements in an overly broad and highly prescriptive manner. Maybe the Commission should have paid more attention to those of us pleading that that item not be rushed forward without greater thought and effort. Unfortunately, I am afraid we are doing the same thing now. While it is critical to ensure the reliability and resiliency of 911 service, this Notice is so deeply flawed that I cannot support it.

First, the Notice proposes to expand the scope of covered 911 providers to nearly every entity that provides 911 capabilities, regardless of whether they have direct contractual relationships with a PSAP. It is so broad that even non-interconnected texting apps could conceivably be brought within the ambit of these rules (although I have no idea what they could certify to in any meaningful way). Yet, these entities had nothing to do with the recent “Sunny Day” outages this item supposedly addresses. Moreover, because the definition of a covered 911 provider is carried forward throughout the rest of the item, a whole host of new requirements would apply to the expanded universe. This sprawling definition taints the entire item in a completely unacceptable way.

Tellingly, the Notice does not even bother to attempt a cost-benefit analysis for this greatly expanded regulatory scheme. Perhaps that is because the current rules are already so burdensome. According to the estimates that the FCC provided to the Office of Management and Budget in order to obtain approval for its existing information collection, the current 911 reliability rules apply to an estimated 1,000 covered 911 service providers, and “each one will incur an average annual burden of approximately 170 hours.” Moreover, the FCC estimated that the rules will create a total in-house cost of over \$14 million annually.

Second, the Notice proposes overbearing and unnecessary entry certifications and exit approvals, as well as a notice regime for “major changes”, and would even apply these requirements to non-carriers. For decades, the Commission has worked to streamline such regulation for carriers. Yet the Notice does not even mention, much less attempt to distinguish, this precedent. And the idea that we would impose such rules on non-carriers, including over-the-top providers, shows that the Commission is seriously reconsidering its traditional, light touch approach for these services.

Third, the concept of 911 Network Operations Center (NOC) providers seems completely unworkable. I understand that this proposal has been described benignly as carriers “sharing a heartbeat” during emergencies. But this is not what the Notice says and the regime designed was not presented accurately to carriers who were briefed. Instead, the Notice proposes to require all covered 911 providers to share information on their networks to the 911 NOC (typically, the incumbent LEC) who may, in some cases, be their competitor. Moreover, the 911 NOC, who does not appear to be compensated for this new role, could be tasked with additional responsibilities, such as “addressing cybersecurity risks in 911 networks”.

Fourth, I continue to believe that the Commission lacks legal authority for these requirements, especially with respect to non-carriers. The Notice points to a couple statutes that provide targeted authority for specific 911 issues and reads them together to provide expansive authority – as if the whole can be more than the sum of its parts. This is simply untrue. The proposal on ancillary authority is just

preposterous and should be rejected. In the end, we should accept a simple fact: statutes mean what they say and say what they mean.

Finally, I continue to believe that these items are a distraction from what should be our priority: moving quickly to NG911 and the public safety benefits that will bring. Indeed, rather than issue a Policy Statement that is needlessly full of hyperbole and is patently misguided to lack any real value, I would prefer that the Commission commit itself fully to NG911.

Separate from the particular problems just identified, it is clear from this overall effort that the real goal is not to solve the challenge at hand to the extent needed, but instead capture any and all market participants in an overly prescriptive and unnecessarily regulatory labyrinth. The item harkens back to an earlier time where competition didn't exist, as if that were a realistic direction we should be going towards. The global marketplace is much more complex than ever before and problems are going to occur despite everyone's best efforts. Unfortunately, the steps proposed in this item would only add more costs to providers, and ultimately consumers, for little to no benefit.