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

In the Matter of	)	
	)	
Improving 911 Reliability	)	PS Docket No. 13-75
	)	
Reliability and Continuity of Communications Networks, Including Broadband Technologies	)	PS Docket No. 11-60
	)	

REPORT AND ORDER

Adopted: December 12, 2013 **Released: December 12, 2013**

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

TABLE OF CONTENTS

APPENDIX A - List of Commenters
APPENDIX B - Final Rules
APPENDIX C - Final Regulatory Flexibility Analysis

I. INTRODUCTION

1. In this *Report and Order*, the Federal Communications Commission (FCC or Commission) adopts rules to improve the reliability and resiliency of 911 communications networks nationwide by requiring that 911 service providers take reasonable measures to provide reliable 911 service, as evidenced by an annual certification. Providers can comply with this requirement by either implementing certain industry-backed "best practices" we adopt today, or by implementing alternative measures that are reasonably sufficient to ensure reliable 911 service. We also require 911 service providers to provide public safety answering points (PSAPs) with timely and actionable notification of 911 outages.

2. This action follows the devastating impact many of these networks experienced as a result of the unanticipated "derecho" storm in June 2012.[1] This storm swiftly struck the Midwest and Mid-Atlantic United States, leaving millions of Americans without 911 service and revealing significant, but avoidable, vulnerabilities in 911 network architecture, maintenance, and operation. After a comprehensive inquiry into the causes of 911 outages during the derecho, as well as 911 network reliability more generally, the Public Safety and Homeland Security Bureau (PSHSB or Bureau) determined that many of these failures could have been mitigated or avoided entirely through implementation of network-reliability best practices and other sound engineering principles.[2]

3. In adopting these rules, we seek to maximize flexibility and account for differences in network architectures without sacrificing 911 service reliability. Accordingly, service providers may certify annually that they have implemented certain industry-backed "best practices" that we adopt herein, or that they have taken alternative measures reasonably sufficient in light of the provider's particular facts and circumstances to ensure reliable 911 service so long as they briefly describe such measures and provide supporting documentation to the Commission. Similarly, service providers may respond by demonstrating that a particular certification element is not applicable to their networks, but they must include a brief explanation of why the element does not apply.

4. The measures we adopt today are based on best practices developed by the Communications Security, Reliability, and Interoperability Council (CSRIC), with refinements designed to add clarity and specific guidance regarding how those practices should be implemented in the context of 911 networks. The certification standards we adopt today are based on best practices identified by CSRIC as critical[3] or highly important,[4] indicating that they significantly reduce the potential for a

[1] The National Weather Service defines a derecho as "a widespread, long-lived wind storm that is associated with a band of rapidly moving showers or thunderstorms. Although a derecho can produce destruction similar to that of tornadoes, the damage typically is directed in one direction along a relatively straight swath. As a result, the term 'straight-line wind damage' sometimes is used to describe derecho damage. By definition, if the wind damage swath extends more than 240 miles (about 400 kilometers) and includes wind gusts of at least 58 mph (93 km/h) or greater along most of its length, then the event may be classified as a derecho." Robert H. Johns, Jeffry S. Evans, & Stephen F. Corfidi, *About Derechos*, NOAA-NWS-NCEP STORM PREDICTION CTR. (Nov.7, 2012), http://www.spc.noaa.gov/misc/AbtDerechos/derechofacts.htm.

[2] *See* FCC PUB. SAFETY & HOMELAND SEC. BUREAU, IMPACT OF THE JUNE 2012 DERECHO ON COMMUNICATIONS NETWORKS AND SERVICES: REPORT AND RECOMMENDATIONS at 3-4 (PSHSB, rel. Jan. 10, 2013), *available at* http://www.fcc.gov/document/derecho-report-and-recommendations (*Derecho Report*).

[3] Best practices categorized as critical are those that CSRIC assessed as being most vital to communications network operators, service providers, equipment suppliers, property managers, and public safety authorities, and that "[s]ignificantly reduce the potential for a catastrophic failure of critical communications network infrastructure and/or services (*e.g.*, telecommunication, public safety, energy sector, financial, etc.)." *See* CSRIC II Working

(continued….)

catastrophic failure of communications or – at a minimum – improve the likelihood of emergency call completion.

5. Based on the information included in the certifications, we may require remedial action to correct vulnerabilities in a service provider's 911 network if we determine that (a) the service provider has not, in fact, adhered to the best practices incorporated in our rules or, (b) in the case of providers employing alternative measures, that those measures were not reasonably sufficient to mitigate the associated risks of failure in one or more of these three key areas. We delegate authority to the Bureau to review certification information and follow up with service providers as appropriate to address deficiencies revealed by the certification process.

6. Finally, we amend our outage reporting rules under Part 4 to clarify Covered 911 Service Providers' obligations to provide PSAPs with timely and actionable notification of outages affecting 911 service. As with the *Notice of Proposed Rulemaking* (*NPRM*) preceding this item, today's *Report and Order* continues to "build[] on the Commission's previous efforts to ensure that the public has access to a state-of-the-art, reliable, and resilient 911 communications system."[5]

II. BACKGROUND

A. 911 Network Architecture

7. The primary function of the 911 network is to route emergency calls to the geographically appropriate PSAP based on the caller's location.[6] When a caller dials 911 on a wireline telephone, the call goes to the local switch serving that caller, as is typical with any other call. The local switch then sends the call to an aggregation point called a selective router, which uses the caller's phone number and address to determine the appropriate PSAP to which the call should be sent.[7] Calls to 911 from wireless phones flow through a switch called a mobile switching center before reaching the selective router. For wireless calls, the sector of the cell tower serving the call provides the approximate location of the caller and is used to determine to which PSAP the call is sent. To complete the call, a connection is set up between the selective router and the appropriate PSAP, typically through a central office serving that PSAP.

8. Once a 911 call reaches the appropriate PSAP, the PSAP queries an automatic location information (ALI) database to determine the location of the caller.[8] For wireline calls, ALI is based on

(Continued from previous page)
Group 6, Best Practice Implementation Final Report at 7-8 (Jan. 2011), *available at* http://transition.fcc.gov/pshs/docs/csric/WG6-Best-Practice-Implementation-Final-Report.pdf.

[4] Highly important best practices include those that, among other things, improve the likelihood of emergency call completion, with caller information, to the appropriate response agency, ensuring access to emergency communications for all callers. *Id.*

[5] *See* In the Matter of Improving 911 Reliability; Reliability and Continuity of Communications Networks, Including Broadband Technologies, PS Docket No. 13-75, PS Docket No. 11-60, *Notice of Proposed Rulemaking*, 28 FCC Rcd 3414, 3415 ¶ 3 (March 20, 2013) (*911 Reliability NPRM*).

[6] *See Derecho Report* at 25.

[7] *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 ("Selective Routing is the ability of the network to select the appropriate destination PSAP for a 9-1-1 call based on the location associated with the caller's [automatic number information (ANI)]. It allows the 9-1-1 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.").

[8] Even if 911 calls originate in the same jurisdiction where they are answered, an ALI database may serve many PSAPs in multiple states. *See* NENA Reply Comments at 2 n.5 ("Many database links, for example, now connect with widely dispersed data centers in Colorado, Florida, Maryland, Washington, etc., regardless of where a 9-1-1 (continued….)

the address associated with the caller's phone number. For wireless calls, providers use various technologies to determine the caller's location. Because ALI is passed to the PSAP along a different path than the one carrying 911 calls, it is possible for a PSAP to lose ALI links without losing 911 service completely.

9. The 911 network architecture described above is evolving from a circuit-switched network to a Next Generation 911 (NG911) network based on Internet protocol (IP) technology. As the Bureau observed in the *Derecho Report*, NG911 networks "offer[] certain advantages over legacy technologies, including greater redundancy and reliability, the ability to provide more useful information for first responders, wider public accessibility (including to those with disabilities), and enhanced capabilities for sharing data and resources among emergency responders."[9] As described in more detail below, we intend today's rules to apply to current 911 networks, as well as NG911 networks to the extent they provide functionally equivalent capabilities to PSAPs. Nevertheless, we undertake to review these rules in five years to make any changes that may be necessary in light of our subsequent experience and future developments with respect to the NG911 transition.[10]

B. FCC Approach to Communications Reliability

10. The Commission has generally approached communications reliability issues by working with service providers to develop voluntary best practices and by measuring the effectiveness of those best practices through outage reporting.[11] For example, federal advisory committees such as CSRIC, which includes representatives from both industry and public safety organizations, have developed numerous network-reliability best practices that communications providers have been encouraged to adopt on a voluntary basis. Since 1992, the Commission has turned to CSRIC and its predecessors, the Network Reliability and Interoperability Council (NRIC) and Media Security and Reliability Council (MSRC), to make recommendations on communications network and system reliability and security.[12] Because of the collaborative and consensus-based nature of this process, CSRIC's best practices generally involve aspects of service that providers have indicated they were already adopting consistently.

11. The Commission's mandatory Network Outage Reporting System (NORS)[13] and voluntary Disaster Information Reporting System (DIRS)[14] provide outage data that help gauge whether

(Continued from previous page)
call originates or terminates."); Comments of Pennsylvania Public Utility Commission at 10 n.8 (Pennsylvania PUC Comments) (citing 911 network functionalities, including delivery of ALI, across state boundaries).

[9] *Derecho Report* at 43-44. The report further found that "[h]ad these NG911 architectures and capabilities been in place in the affected areas, they likely could have significantly lessened the derecho's impact on emergency communications." *Id.* at 44.

[10] *See* FCC, LEGAL AND REGULATORY FRAMEWORK FOR NEXT GENERATION 911 SERVICES: REPORT TO CONGRESS AND RECOMMENDATIONS § 3.1.2 (Feb. 22, 2013), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-319165A1.pdf.

[11] *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 (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).

[12] CSRIC's mission is to provide recommendations to the FCC to ensure, among other things, security and reliability of communications systems, including telecommunications, media, and public safety. It is a multi-stakeholder, public-private process that includes communications providers, public safety entities, state and local governments, tribal entities, consumer groups, and federal government agencies. CSRIC was first established in 2007 and has been re-chartered for additional two-year terms in 2009, 2011, and 2013; each iteration is informally referred to as CSRIC I, CSRIC II, CSRIC III, etc. Each CSRIC is divided into discrete working groups, which make recommendations on particular topics for adoption by the full CSRIC.

[13] NORS is the Commission's mandatory web-based filing system through which communications providers
(continued….)

best practices have been implemented in certain circumstances or service areas, but the Commission has not required service providers to implement these practices. From time to time, however, the Bureau has publicly reminded 911 service providers of the importance of following industry-developed best practices in light of outage trends suggesting to the Bureau that they have not been implemented adequately.[15] The Bureau also works with service providers on an informal basis to identify and resolve communications reliability issues revealed through the outage reporting process.

12. In 2006, the Commission established the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks (Katrina Panel) to make recommendations to the Commission regarding ways to improve disaster preparedness, network reliability and communications among first responders.[16] In 2007, acting on the findings of the Katrina Panel, the Commission adopted rules requiring certain communications providers to maintain minimum levels of backup power for central offices, cell sites, and other network assets.[17] Another rule adopted in the *Katrina Panel Order*, requiring local exchange carriers, wireless service providers subject to 911 requirements, and interconnected VoIP service providers "to conduct an analysis of the resiliency and reliability of their 911 networks or systems and to submit a report to the Commission,"[18] was implemented by the Bureau in

(Continued from previous page)
covered by the Part 4 outage reporting rules (*e.g.*, wireline, wireless, cable) must submit reports to the FCC. These reports are presumed confidential to protect sensitive and proprietary information about communications networks. *See* 47 C.F.R. § 4.2. The NORS system uses an electronic template to promote ease of reporting and encryption technology to ensure the security of the information filed. PSHSB's Cybersecurity and Communications Reliability Division administers NORS, monitors the outage reports submitted through NORS, and performs analyses and studies of the communications disruptions reported. Generally, a NORS report must be filed when the effects of an outage reach a certain threshold (*e.g.*, lasting at least thirty minutes and potentially affecting 900,000 user-minutes). Then, the filing party has up to thirty days to supplement the filing with more complete information. *See* 47 C.F.R. § 4.1 *et seq.; see also Network Outage Reporting System (NORS)*, FCC, http://transition.fcc.gov/pshs/services/cip/nors/nors.html.

[14] DIRS is a voluntary, web-based system that communications companies, including wireless, wireline, broadcast, and cable providers, can use to report communications infrastructure status and situational awareness information during times of crisis. When there is a full activation of DIRS, participants are generally excused from making submissions in NORS. *See Disaster Information Reporting System (DIRS)*, FCC, http://transition.fcc.gov/pshs/services/cip/dirs/dirs.html. As with NORS, information submitted into DIRS is presumed confidential but may be shared with federal agencies such as the Department of Homeland Security on a confidential basis. *See* The FCC's Public Safety and Homeland Security Bureau Launches Disaster Information Reporting System (DIRS), *Public Notice*, DA 07-3871 (PSHSB 2007).

[15] *See* FCC's Public Safety and Homeland Security Bureau Reminds Telecommunications Service Providers of Importance of Implementing Established 911 and Enhanced 911 Services Best Practices, *Public Notice*, DA 12-891, 27 FCC Rcd 6085 (PSHSB rel. June 6, 2012) (*2012 Best Practices PN*); FCC's Public Safety and Homeland Security Bureau Reminds Telecommunications Service Providers of Importance of Implementing Advisory Committee 911 and Enhanced 911 Services Best Practices, *Public Notice*, DA 10-494, 25 FCC Rcd 2805 (PSHSB rel. March 24, 2010) (*2010 Best Practices PN*).

[16] *See* In the Matter of Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, EB Docket No. 06-119, WC Docket No. 06-63, *Order*, 22 FCC Rcd 10541, 10542 ¶ 4 (2007) (*Katrina Panel Order*).

[17] *See* In the Matter of Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, EB Docket No. 06-119, WC Docket No. 06-63, *Order on Reconsideration*, 22 FCC Rcd 18013, 18035, App. B (2007). These backup power rules, however, were the subject of judicial challenge by several wireless providers and never took effect. They were ultimately vacated by the U.S. Court of Appeals for the District of Columbia Circuit after the Commission notified the court of its intent to adopt revised backup power rules in further rulemaking proceedings. *See CTIA - The Wireless Association v. FCC*, No. 07-1475 (D.C. Cir. filed July 31, 2009).

[18] *See Katrina Panel Order*, 22 FCC Rcd at 10572 ¶ 99 (2007). This requirement was codified in Part 12 of the Commission's rules, and delegated authority to the Bureau to establish the specific data required in each report, but
(continued….)

2009 when it requested general information from service providers about 911 architecture in the United States. As we noted in the *911 Reliability NPRM*, however, these reports proved of limited use, lacking the specificity necessary to determine network reliability in individual cases.[19]

13. In 2011, the Commission released a *Notice of Inquiry* (*Reliability NOI*) in PS Docket No. 11-60, which sought comment on the reliability, resiliency, and continuity of our nation's communications networks, including broadband technologies.[20] Among other topics, the *NOI* inquired about "the ability of communications networks to provide continuity of service during major emergencies, such as large-scale natural and man-made disasters."[21] The Commission emphasized that "[p]eople dialing 911, whether using legacy or broadband-based networks, must be able to reach emergency personnel for assistance."[22]

14. Service providers responding to the *Reliability NOI* assured the Commission that they had infrastructure and plans in place to maintain continuity of communications in the event of severe weather, loss of commercial power, and other emergency conditions. The United States Telecom Association (U.S. Telecom), for example, commented that its members "have voluntarily spent hundreds of millions of dollars and countless hours preparing for disaster recovery in order to support continued quality service to their customers, even during emergencies."[23] Similarly, Verizon asserted that its "legacy voice, wireless, and broadband networks have significant redundancy and other protective measures in place to keep the networks up or to quickly restore them during disasters and severe overloads."[24] Accordingly, service providers urged the Commission to continue promoting voluntary best practices in lieu of regulatory obligations regarding circuit diversity, backup power, and other aspects of network reliability.[25]

C. June 2012 Derecho

15. On June 29, 2012, a fast-moving derecho storm brought a wave of destruction across wide swaths of the United States, beginning in the Midwest and continuing through the Appalachians and Mid-Atlantic states until the early morning of June 30. The derecho resulted in twenty-two deaths and

(Continued from previous page)
provided that "these reports should include descriptions of the steps the service providers intend to take to ensure diversity and dependability in their 911 and E911 networks and/or systems, including any plans they have to migrate those networks and/or systems to a next generation Internet Protocol-based E911 platform." 47 C.F.R. § 12.3(a).

[19] For example, the reports did not provide sufficient information to assess whether 911 service providers were implementing diversity in their routing of 911 circuits for PSAPs in major metropolitan areas. *See 911 Reliability NPRM*, 28 FCC Rcd at 3427 ¶ 27.

[20] In the Matter of Reliability and Continuity of Communications Networks, Including Broadband Technologies, *et al*., PS Docket No. 11-60, *Notice of Inquiry*, 26 FCC Rcd 5614 (2011) (*Reliability NOI*).

[21] *Id.* at 5615 ¶ 2.

[22] *Id.* at 5616 ¶ 5.

[23] NOI Comments of U.S. Telecom Association at 1 (U.S. Telecom Association NOI Comments)

[24] NOI Comments of Verizon at 2 (Verizon NOI Comments).

[25] *See* Verizon NOI Comments at 12 ("In light of the already-established government resources devoted to understanding the availability of networks during disasters, the Commission should continue to promote the establishment and updating of best practices that providers can adopt to better protect their networks."); U.S. Telecom Association NOI Comments at 4 ("While . . . emergency preparedness efforts can be costly, USTelecom's member companies have continually demonstrated that they have a vested interest – even without a regulatory mandate – in making the investment necessary to ensure the continuity and reliability of their networks during emergencies."); AT&T NOI Comments at 2-3 ("The Commission could best serve the goals of network survivability by supporting the development and dissemination of industry-generated best practices."); CenturyLink NOI Comments at i ("CenturyLink urges the Commission to continue its support for the important voluntary best practices work being done by organizations such as ATIS's NRSC, NRIC and CSRIC.").

widespread property damage, and left millions of residents without electrical power for as long as two weeks.[26]

16. While the destruction caused by the derecho resembled that of other major storms in some respects, it also proved different in others. For example, the landfall of a hurricane is typically predicted days in advance, allowing first responders and communications providers time to prepare. The derecho, however, moved rapidly across multiple states with very little warning. The derecho thus put critical infrastructure to an unexpected test and revealed significant vulnerabilities in service providers' networks and operations.

17. The derecho caused particularly widespread disruptions to 911 services.[27] From isolated breakdowns in Ohio, New Jersey, Maryland, and Indiana, to systemic failures in northern Virginia and West Virginia, a significant number of 911 systems and services were partially or completely down for as long as several days. Across the storm's path, at least seventy-seven PSAPs serving more than 3.6 million people in six states lost some degree of network connectivity, including vital information on the location of 911 callers.[28] At least seventeen 911 call centers in three states lost service completely, affecting the ability of more than two million residents to reach 911.[29] Nearly 9 percent of all PSAPs in the six affected states experienced some loss of service, affecting more than 8 percent of those states' total residents.

18. The effects were particularly severe in northern Virginia, where four PSAPs in the densely-populated National Capital Region lost service completely, and in West Virginia, where eleven PSAPs could not receive 911 calls for as long as twelve hours.[30] Fairfax County, Virginia, for example, notes that the disruption of 911 service it experienced after the derecho "was the longest and most severe 911 outage since Fairfax County implemented Enhanced 911 in 1988," leaving 1.1 million county residents without access to 911 for seven hours and preventing nearly 1,900 911 calls from reaching the Fairfax County PSAP.[31] Other affected PSAPs lost ALI links or had to reroute calls to other jurisdictions.

D. PSHSB Derecho Report

19. Immediately after communications and 911 services were restored, the Bureau began a comprehensive inquiry to determine why each outage occurred and how such problems could be prevented in the future. The Bureau analyzed more than 500 confidential NORS reports containing information on the cause, duration, and resolution of each outage, as well as numerous DIRS reports from the areas hit hardest by the derecho. Bureau staff also interviewed representatives of eight communications providers, twenty-eight PSAPs, three battery manufacturers, one generator manufacturer, and numerous state and county entities. In addition, the Bureau participated in several federal, state, and local meetings and hearings on the effects of the derecho.[32] These interactions clarified and expanded the information the Commission had already received via NORS and DIRS.

---

[26] *See Derecho Report* at 3.

[27] *See, e.g.*, Patricia Sullivan, *911 Failure Affected 2.3 Million in Northern Virginia*, WASH. POST, July 11, 2012.

[28] *Id*.

[29] *Derecho Report* at 4.

[30] *Id.* at 28-34.

[31] Public Notice Comments of Fairfax County, Virginia at 2, 12; *Derecho Report* at 4 (citing Fairfax County Public Notice Comments at 12).

[32] *See Resilient Communications: Current Challenges and Future Advancement: Hearing Before the Subcomm. on Emergency Preparedness, Response, & Commc'ns of the H. Comm. on Homeland Sec.*, 112th Cong. (Sept. 12, 2012) (statement of David S. Turetsky, Chief, Public Safety and Homeland Security Bureau); *Reliability of the District's 911 Call System: Hearing Before the D.C. Council Comm. on the Judiciary* (Sept. 20, 2012) (statement of David S. Turetsky, Chief, Public Safety and Homeland Security Bureau); *COG to Review 911 Outages and Other*

(continued….)

20. On July 18, 2012, the Bureau released a *Public Notice* seeking comment on issues surrounding the derecho, including the cause of the outages, their effect on public safety, and the resiliency and reliability of 911 networks generally.[33] This *Public Notice* focused on actions to ensure dependable 911 service, both now and in an NG911 environment. In response to the *Public Notice*, the Bureau received several dozen comments and reply comments from parties representing a diverse range of interests, including local governments concerned about a pattern of 911 outages[34] and communications providers calling for new voluntary best practices to address problems experienced during the derecho.[35]

21. In its January 2013 *Derecho Report*, the Bureau announced the results of its inquiry and provided specific recommendations for Commission action to improve the reliability and resiliency of 911 networks nationwide. The Bureau found that many communications outages during the derecho, including 911 outages, could have been prevented through implementation of best practices developed by entities such as CSRIC and the Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC).[36] The Bureau found that, above and beyond any physical destruction by the derecho, 911 communications were disrupted in large part because of avoidable planning and system failures, including inadequate physical diversity of critical 911 circuits and a lack of functional backup power in central offices.[37] Links and aggregation points supplying telemetry data to network operations centers (NOCs) also failed, depriving communications providers of visibility into critical network functions.[38] Among other things, the Bureau recommended that the Commission take action to ensure that 911 service providers (1) routinely audit critical 911 circuits for physical diversity, (2) maintain adequate central-office backup power, (3) deploy physically diverse network monitoring links, and (4) provide PSAPs with timely and actionable notification of communications outages.[39]

E. 911 Reliability Notice of Proposed Rulemaking

22. On March 20, 2013, the Commission adopted a *Notice of Proposed Rulemaking* (*911 Reliability NPRM* or *NPRM*) outlining options to implement recommendations from the *Derecho Report*.[40] These options ranged from reporting and certification obligations, to mandatory reliability requirements supported by site inspections and compliance reviews. The *NPRM* noted that the implementation options need not be mutually exclusive and sought comment "on whether each of these approaches can stand alone, or whether the Commission should adopt two or more options as part of an integrated approach."[41] The *NPRM* also proposed to amend the Commission's rules to require 911

(Continued from previous page)
Failures Resulting from "Derecho," METRO. WASH. COUNCIL OF GOV'TS (Jul. 11, 2012), *available at* http://www.mwcog.org/news/press/detail.asp?NEWS_ID=584.

[33] Public Safety and Homeland Security Bureau Seeks Comment On 911 Resiliency and Reliability in Wake of June 29, 2012, Derecho Storm in Central, Mid-Atlantic, and Northeastern United States, PS Docket No. 11-60, *Public Notice*, 27 FCC Rcd 8131 (PSHSB July 18, 2012) (*Derecho Public Notice*).

[34] *See* Fairfax County Comments at 18-20.

[35] *See, e.g.*, Comments of Verizon and Verizon Wireless at 14 (Aug. 17, 2012) (Verizon Public Notice Comments).

[36] The ATIS NRSC "strives to improve network reliability by providing timely consensus-based technical and operational expert guidance to all segments of the public communications industry." *See Network Reliability Steering Committee (NRSC)*, ATIS, http://www.atis.org/NRSC/index.asp (last visited Feb. 19, 2013). The NRSC advises the communications industry through developing and issuing standards, technical requirements, technical reports, bulletins, best practices, and annual reports.

[37] *Derecho Report* at 1.

[38] *See id.* at 18, 21, 40-41.

[39] *See id.* at 39-41.

[40] *See generally 911 Reliability NPRM*, 28 FCC Rcd at 3414.

[41] *Id.* at 3425-26 ¶ 24.

service providers, and other communications providers subject to the existing rule, to notify PSAPs of communications outages "immediately," with specific information about the nature of the outage and area affected.[42] In response to the *NPRM*, we received twenty-nine comments and nine replies representing a broad range of communications providers, trade associations, PSAPs, and public safety organizations.[43]

III. DISCUSSION

A. Need for Commission Action

23. One of the Commission's primary responsibilities is to "make available, so far as possible, to all people of the United States, . . . a . . . wire and radio communication service . . . for the purpose of promoting safety of life and property."[44] Consistent with that overarching obligation, the Commission has specific statutory responsibilities with respect to 911 service.[45] The *911 Reliability NPRM* sought comment "on the appropriate balance between voluntary best practices and Commission mandates"[46] to achieve the Commission's goals with respect to public safety generally and 911 communications specifically. The outage reporting process has often been effective in improving the reliability and resiliency of many communications services, and we continue to support NORS, DIRS, and an emphasis on voluntary best practices and outage reporting in the context of everyday communications. Nevertheless, preventable 911 network failures during the derecho put lives and property at risk and revealed that service providers have not consistently implemented vital best practices voluntarily despite repeated reminders and their past claims to the contrary.[47] In light of this experience and substantial evidence in the record of this proceeding, we conclude that additional Commission action is both warranted and needed with respect to critical 911 communications.

1. Voluntary Measures Alone Have Proven Inadequate

24. The *Derecho Report* found that "911 and other problems could and would have been avoided if providers had followed industry best practices and available guidance," and recommended consideration of "specific action by the Commission to supplement the current best-practice approach in key areas."[48] Service providers argue that they have addressed vulnerabilities revealed by the derecho,[49] and that the Commission should "continue its active support of and participation in the development and refinement of industry best practices for 911 reliability."[50] CenturyLink argues that "[t]he solid performance of most carriers' networks during and after this historic storm demonstrates the industry's strong emphasis and commitment to network reliability absent prescriptive reliability rules."[51] Similarly,

[42] *Id.* at 3442-44 ¶¶ 67-74.

[43] *See* List of Commenting Parties, *infra*, App. A.

[44] 47 U.S.C. § 151.

[45] *See Nuvio Corp. v. FCC*, 473 F.3d 302, 311 (D.C. Cir. 2007) (Kavanaugh, J., concurring). *See also 911 Reliability NPRM*, 28 FCC Rcd at 3444 ¶ 76 (citing 911 statutes).

[46] *911 Reliability NPRM*, 28 FCC Rcd at 3423 ¶ 20.

[47] *See, e.g.*, U.S. Telecom NOI Comments at 1-2; Verizon NOI Comments at 2; AT&T NOI Comments at 3-4; CenturyLink NOI Comments at i.

[48] *Derecho Report* at 1, 39.

[49] *See* Verizon Comments at 3-6; Frontier Comments at 2-4.

[50] AT&T Comments at 1. *See also* ATIS Comments at 6 ("Unlike regulatory mandates, which generally impose rigid rules based an evaluation of circumstances at a specific point in time, Best Practices provide guidance based on industry expertise and experience and continually evolve to meet new technical, business, and consumer expectations."); US Telecom Comments at 2 ("The Commission thus should direct the existing Industry Forums to determine whether modified or additional best practices are warranted in light of the lessons learned from the Derecho.").

[51] CenturyLink Reply Comments at 2.

the Telecommunications Industry Association supports a "reliability ecosystem" based on "voluntary and consensus-based standards, best practices, self-evaluation efforts, and public-private partnership efforts."[52] Although these comments reflect the general philosophy that the Commission has applied to communications reliability in the past, we have concluded, based on our repeated experiences, the findings in the *Derecho Report*, and the record in this proceeding, that a purely voluntary approach to 911 reliability has not been sufficiently effective.

25. PSHSB twice issued *Public Notices* reminding 911 service providers to adhere to best practices based on outage reports indicating those practices have not been implemented consistently, particularly with regard to circuit diversity. In 2010, the Bureau noted that "[t]hrough an examination of network outage reports filed through [NORS], the Bureau has observed a significant number of 911/E911 service outages caused by a lack of diversity that could have been avoided at little expense to the service provider."[53] In 2012, *less than one month before the derecho*, PSHSB again stated that "[b]ased on submissions in [NORS] and publicly available data, the Bureau has observed a number of major 911/E911 service outages caused by inadequate diversity and/or the failure to maintain diversity."[54] The Bureau added that "[m]ost of these major outages could have been prevented if existing NRIC best practices had been followed."[55] Despite the promulgation by industry of these best practices and two formal, public reminders to comply with them more consistently, the derecho revealed multiple instances of insufficient circuit diversity resulting in 911 outages.[56] Likewise, widespread backup power and network monitoring failures during the derecho could have been avoided had affected service providers more consistently adhered to relevant best practices.

26. Similarly, in 2011 the Bureau urged the ATIS NRSC to develop recommendations to prevent failure of centralized automatic message accounting (CAMA) 911 trunks during mass call events, such as the spikes in 911 calling from natural disasters.[57] This work was undertaken following multiple mass call events that caused disruptions in 911 service.[58] This process led to publication of a detailed report on how to prevent CAMA trunks from mistakenly being removed from service during mass call events.[59] During the derecho, two service providers that implemented only some of the ATIS NRSC recommendations, or none at all, reported CAMA trunk throughput issues that degraded 911 service to three PSAPs in three states, whereas other service providers that adopted all of the ATIS NRSC recommendations performed better.[60] In light of this evidence, the Bureau concluded that the affected PSAPs would have received more 911 calls had their service providers implemented those

[52] Telecommunications Industry Association Comments at 4.

[53] *2010 Best Practices PN*, 25 FCC Rcd at 2806.

[54] *2012 Best Practices PN*, 27 FCC Rcd at 6085.

[55] *Id.*

[56] *See, e.g. Derecho Report* at 29 (noting that a diversity audit by Verizon could have revealed single points of failure that disrupted 911 service to the Fairfax County, Virginia, PSAP).

[57] CAMA trunks are a legacy technology used to route 911 calls to PSAPs in many jurisdictions. During times when a PSAP receives a large volume of calls, a timing mismatch between the selective router and the customer premises equipment at the PSAP can result in trunks being taken out of service even though these trunks have not failed. This reduces a 911 network's capacity to route calls to the appropriate PSAP.

[58] *See, e.g.*, Todd Shields, *Verizon Asked to Probe 'Alarming' Dropped 911 Calls*, BLOOMBERG, Feb. 18, 2011, http://www.bloomberg.com/news/2011-02-18/fcc-asks-verizon-about-alarming-number-of-dropped-911-calls-in-snowstorm.html.

[59] *See* NRSC 911 CAMA TRUNK THROUGHPUT OPTIMIZATION ANALYSIS (ATIS-0100034) (rel. Aug. 2011), *available at* http://www.atis.org/legal/Docs/NRSC/CAMATrunk_Transmittal_Final.pdf.

[60] *See Derecho Report* at 27, 32, 33 (discussing CAMA trunk issues at PSAPs served by CenturyLink and Frontier).

recommendations more fully.[61] These experiences have demonstrated the primary shortcoming of the voluntary approach: service providers may choose – and have chosen – to disregard these voluntary recommendations, even when they concern critical 911 services. This is unacceptable.

27. Comments from PSAPs, government entities, and public safety groups validate our concerns that the status quo is unacceptable and unlikely to improve adequately through voluntary measures alone. The National Emergency Number Association (NENA), for example, states that "the long-established practice of deferring to carriers' and system service-providers' assurances with respect to voluntary implementation of 'best practices' has not produced the intended outcome."[62] The Association of Public-Safety Communications Officials (APCO) agrees that a voluntary approach "has proven inadequate."[63] Fairfax County, Virginia – one of the jurisdictions hardest-hit by the derecho and one of the largest and most sophisticated PSAPs in the country – has concluded based on its experience that "[r]elying solely on voluntary compliance does not work."[64]

28. In light of these concerns and the preventable 911 outages discussed above, we are not persuaded by service providers' arguments that "the Commission may not need to take any formal regulatory action at this time."[65] The avoidable 911 failures during the derecho were not for a lack of guidance from industry or from the Commission. Relevant best practices regarding circuit diversity, backup power, and network monitoring were widely available, but multiple service providers failed to implement them effectively, with serious consequences to public safety. Our conclusion, based on outage reports and the experiences in the derecho, and that of affected PSAPs, is that the discharge of our statutory responsibility for promoting the safety of life and property no longer justifies relying solely on the implementation of key best practices on a voluntary basis.

29. Furthermore, we disagree with service providers' arguments that "competitive market forces already drive communications providers to follow industry best practices and to invest in their networks to ensure continuity and restoration of communications, especially 911 communications."[66] While competitive pressures may drive investment in reliability of communications services marketed to businesses and consumers, most PSAPs and 911 authorities have a limited choice of 911 service providers and cannot realistically switch to a competitor if they are unhappy with their service. Nor is there typically transparency for PSAP customers with regard to the reliability practices addressed in this proceeding. NENA, for example, notes that "[u]nder a tariff regime, 911 authorities are often faced with a take-it-or-leave-it offering, with no room for further negotiation."[67] It adds that "the high capital cost of establishing independent 911 service and ongoing consolidation in the 911 services market have left 911 authorities with limited market power, and established dangerous opportunities for vendor lock-in scenarios."[68]

---

[61] *See id.* at 32-33.

[62] NENA Comments at 2-3.

[63] APCO Comments at 2.

[64] Fairfax County Comments at 2.

[65] Frontier Comments at 5.

[66] AT&T Comments at 3-4.

[67] NENA Comments at 8.

[68] *Id.* at 9. While adoption of NG911 is likely to offer PSAPs greater choice in 911 capabilities and service providers, and may warrant revisiting our rules in the future, that competitive marketplace does not exist now, and we are unable to predict when or how it might arrive. *See id* at 7 (observing that "the long-term trend is toward . . . greater unbundling of 911 service provisioning, and toward more competitive markets"). Given the serious consequences of 911 service failures, and in light of our experiences, we believe we cannot rely solely on the future promise of NG911 to address the problem.

30. We also reject the suggestion that Commission action to improve 911 reliability would "disrupt the development of Best Practices through a heavy-handed reclassification of Best Practices as regulatory mandates."[69] This is a red herring. The approach we adopt today is not "heavy-handed" or overly prescriptive, but rather flexible and designed to encourage innovation. It allows service providers to certify compliance either with specific best practices based on standards already established through industry consensus, or with reasonable alternatives shown to be appropriate in their circumstances. We support the continued development of new best practices and modification of existing best practices, but we are not persuaded that additional voluntary measures alone would provide adequate assurance of a reliable and resilient 911 system.

2. 911 Reliability is a Nationwide Concern

31. Finally, some commenters suggest that 911 outages during the derecho were isolated incidents involving a small number of service providers that do not accurately reflect the reliability of 911 networks nationwide.[70] AT&T, for example, comments that "[t]he *Derecho Report* did not identify systemic flaws in 911 communications networks that warrant industry-wide regulatory remedies or the adoption of new regulation[s]."[71] Another commenter argues that carriers identified in the *Derecho Report* and *911 Reliability NPRM* should be subject to Commission action, but that expanding reliability rules beyond those carriers would be unduly burdensome without a demonstrated need.[72]

32. In contrast, public safety commenters contend that the derecho revealed vulnerabilities in 911 infrastructure that exist nationwide.[73] NENA, for example, comments that "[b]ased on anecdotal evidence from PSAP and 911 authority personnel around the country, NENA believes that the members of the carrier and SSP community mentioned by name in the *Derecho Report* are not exceptional cases."[74] NATOA further comments that "[w]e believe that it is important to have reliability standards that are applicable and actionable nationwide, regardless of the specific region."[75]

33. In light of our inquiry following the derecho and our ongoing experience with outage reporting, we agree that 911 reliability is a nationwide issue involving more than one region or service provider. Since we established NORS in 2004, service providers have submitted nearly 6,000 outage reports involving disruption of E911 service capabilities as of June 2013. These reports have originated from every state in the nation, and there is no indication that the region affected by the derecho accounts for more than its share of 911 outages. Indeed, approximately 81 percent of E911 outages reported in NORS have occurred outside the six states most affected by the derecho.[76] Furthermore, the *Derecho Report* identified preventable 911 failures by not one, but four, of the nation's largest 911 service providers,[77] which together serve a vast majority of Americans.[78]

---

[69] *See* ATIS Comments at 6.

[70] *See* Western Telecommunications Alliance Comments at 3-4 ("Whereas the slow and painful recovery from the derecho took place in full view of the Commission and other federal government officials, it must be emphasized that it was a unique and localized event that should not serve as the basis for nationwide policy and regulatory changes.").

[71] AT&T Comments at 3.

[72] *See* Blooston Rural Carriers Comments at 2-5.

[73] *See* NENA comments at 3 ("NENA believes that the states of the networks that failed as a result of the derecho are broadly representative of the states of carrier and SSP networks nation-wide.").

[74] NENA Comments at 3.

[75] NATOA Comments at 3.

[76] *See Derecho Report* at 27 (describing 911 outages in Virginia, West Virginia, Ohio, New Jersey, Maryland, and Indiana).

[77] *See id.* at 12 (citing PSAPs served by Verizon, Frontier, CenturyLink, and AT&T).

34. Some commenters suggest that improved 911 performance in subsequent events such as Superstorm Sandy shows that problems revealed by the derecho have been resolved,[79] but the derecho was unlike a hurricane in many respects. As the *Derecho Report* observed, "derechos are more like earthquakes, tornados, and man-made events for which there is little-to-no advance notice and opportunity to prepare."[80] The landfall of Superstorm Sandy, by contrast, was anticipated for several days and gave service providers time to test equipment, stage critical assets, and adjust staffing levels. Verizon, for example, notes in a filing with New York State regulators that it began implementation of its "emergency preparedness plan" on October 25, 2012, four days before the storm's October 29 landfall.[81] Thus, while it is fortunate that the 911 outages caused by the derecho have not recurred since, our experience, coupled with the widespread nature of the problems identified in the *Derecho Report* and the record in this proceeding, leads us to conclude that there is a substantial risk of similar failures in the future, and it would not be a prudent exercise of our statutory responsibilities to wait and see.

35. That said, we recognize that 911 service providers in different parts of the nation have been affected to varying degrees by recent events and face diverse reliability challenges due to weather, geography, population density, and other factors.[82] The certification approach we adopt today reflects the fact that, while all Americans have an expectation of reliable 911 service, appropriate actions to improve and maintain reliability may vary by service provider and location.

B. Entities Subject to Rules

36. The *911 Reliability NPRM* sought comment on the parties to which the proposals contained therein would apply.[83] The certification rules we adopt today will apply to every "Covered 911 Service Provider," defined as any entity that provides 911, E911, or NG911 capabilities such as call routing, ALI, ANI, or the functional equivalent of those capabilities, directly to a PSAP, statewide default answering point, or appropriate local emergency authority,[84] or that operates one or more central offices

(Continued from previous page)

[78] Of the seventy-seven PSAPs that experienced some disruption of 911 service during the derecho, seventeen served by Verizon and Frontier lost 911 service completely, while four PSAPs served by AT&T experienced intermittent ALI outages and three PSAPs served by CenturyLink had CAMA trunk problems or ALI difficulties. *See id.* at 32-35. *But see* AT&T Comments at 6 n.2 ("Whether intended or not, the *Derecho Report* gives readers the false impression that AT&T Ohio lost ALI capability for nearly four days. In reality, AT&T Ohio experienced limited, intermittent failures on ALI links over a four-day period during and after the storm, which AT&T Ohio addressed by rerouting traffic to alternative PSAPs. But no PSAP in Ohio—at least that AT&T Ohio serves—lost ALI capability for a period of four days.").

[79] *See* Verizon Comments at 1-2 ("These improved practices contributed to a positive network experience during Hurricane Sandy, during which 911 problems were generally avoided in the New Jersey and New York areas affected most heavily."); Frontier Comments at 5 (arguing that "carriers like Frontier have embraced the lessons learned from the derecho and the changes have shown successful in Superstorm Sandy").

[80] *Derecho Report* at 1.

[81] *See* Report of Verizon New York Inc. Concerning Its Performance in Response to Hurricane Sandy, attached to Letter from Richard C. Bozsik, Director – Regulatory – Verizon New York, to Chad G. Hume, Director, Office of Telecommunications, New York State Department of Public Service, NYPSC Case No. 13-M-0025 (Apr. 19, 2013), *available at* http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={59414447-CD1C-47D0-B351-F4C7947EEB57}.

[82] *See, e.g.*, AT&T Reply Comments at 6 (arguing that prescriptive regulation "runs the risk of reducing 911 reliability by depriving providers of the flexibility needed to tailor network reliability practices to their unique networks and the physical environments in which they are deployed").

[83] *911 Reliability NPRM*, 28 FCC Rcd at 3425 ¶ 23.

[84] FCC rules define "[a]ppropriate local emergency authority" as "[a]n emergency answering point that has not been officially designated as a Public Safety Answering Point (PSAP), but has the capability of receiving 911 calls and either dispatching emergency services personnel or, if necessary, relaying the call to another emergency service (continued….)

that directly serve a PSAP.[85] For purposes of these rules, a central office "directly serves a PSAP" if it (1) hosts a selective router or ALI/ANI database (2) provides functionally equivalent NG911 capabilities, or (3) is the last service-provider facility through which a 911 trunk or administrative line passes before connecting to a PSAP. This definition encompasses entities that provide capabilities to route 911 calls and associated data such as ALI and ANI to the appropriate PSAP, but *not entities that merely provide the capability for customers to originate 911 calls*.[86]

37. The definition of "Covered 911 Service Provider" that we adopt reflects the fact that, while most current 911 networks rely on the infrastructure of an incumbent local exchange carrier (ILEC), no single type of entity will always provide 911 service in every community. In addition, the transition to an Internet protocol (IP) architecture for NG911 services will allow an expanded range of entities beyond ILECs to route and deliver 911 calls, as well as location and callback information, to local PSAPs or consolidated call centers. Consistent with the goals of the Next Generation 911 Advancement Act of 2012,[87] the Commission seeks to promote NG911 adoption and account for changing technologies that support these functions while ensuring that legacy 911 infrastructure remains reliable as long as it is in use. We also recognize that overbroad rules could inadvertently impose obligations on entities that provide peripheral support for NG911 but may not play a central role in ensuring 911 reliability or benefit as much as a typical circuit-switched ILEC from the best practices discussed below. To minimize the risk of unintended effects, we describe covered entities in terms of the core 911 capabilities they provide rather than the technology they employ or how they are currently classified under our rules.

38. Commenters generally agree with the *911 Reliability NPRM's* focus on entities that route 911 calls and number or location information to PSAPs, rather than the broader class of entities that allow customers to originate 911 calls.[88] The American Cable Association, for example, states that "the

(Continued from previous page)
provider. An appropriate local emergency authority may include, but is not limited to, an existing local law enforcement authority, such as the police, county sheriff, local emergency medical services provider, or fire department." *See* 47 C.F.R. § 64.3000(b); 47 C.F.R. § 20.3. Where appropriate local emergency authorities act as the functional equivalent of PSAPs by receiving and dispatching 911 calls, their service providers are Covered 911 Service Providers. We do not intend this definition to extend to entities that provide *non-911* communications services to local emergency authorities.

[85] Specific basic 911 and E911 capabilities are defined elsewhere in the Commission's rules. *See* 47 C.F.R. § 64.3000 et seq. (obligation to transmit 911 calls and transition to 911 as the universal emergency telephone number). Because NG911 continues to evolve and may offer additional functionality in the future, we decline to adopt a comprehensive definition of NG911 capabilities at this time. The rules we adopt today apply to capabilities provided over NG911 networks to the extent those capabilities are functionally equivalent to current 911 and E911 capabilities.

[86] We focus on network connectivity to PSAPs rather than on call origination in this *Report and Order* because the derecho and other events have shown that failure of critical infrastructure involved in routing and delivering 911 calls and ALI may cause outages affecting an entire community regardless of the technology or service provider each resident uses to dial 911. We also note that we are addressing call origination and reliability of other communications services during emergencies in a separate proceeding regarding transparency of performance for wireless networks. *See* In the Matter of Improving the Resiliency of Mobile Wireless Communications Networks; Reliability and Continuity of Communications Networks, Including Broadband Technologies, PS Docket Nos. 13-239, 11-60, *Notice of Proposed Rulemaking*, FCC 13-125 (Sept. 27, 2013), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0927/FCC-13-125A1.pdf..

[87] Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96 (2012), Title VI, Subtitle E §§ 6501 et seq.

[88] *See, e.g.*, ATIS Comments at 8-9 (stating that "the relevant part of the network that is being addressed in this proceeding is the final leg into the PSAP," and that this definition "should be exclusively limited to the provider from whom the PSAP purchases services"); AT&T Comments at 2 (*if* the Commission were to adopt any regulatory scheme, it should apply uniformly to all communications providers responsible for routing and delivering 911 calls to PSAPs).

Commission should make sure to define the term '911 service provider' to include only entities providing communications services directly to PSAPs under tariff, contract or other direct arrangement and exclude providers who only provide 911 service to their customers."[89]

39. Some commenters, however, suggest that the proposed rules should extend further, to backhaul providers that transport 911 calls,[90] data centers that provide NG911 capabilities,[91] and even to PSAPs and consumers.[92] We decline to expand our definition as far as these commenters suggest. Under current network configurations, while many service providers may play some role in the origination and delivery of individual 911 calls, only a limited number of entities provide 911 connectivity directly to PSAPs. Thus, we do not intend today's rules to apply to wireless providers, VoIP providers, backhaul providers, Internet service providers (ISPs), or commercial data centers based on the functions they currently provide in 911 networks, assuming they do not provide the functions of a Covered 911 Service Provider under our definition.

40. While some commenters, particularly rural local exchange carriers (RLECs), advocate explicit exemptions from 911 reliability rules for certain parties,[93] we intend the certification requirement adopted here to apply to all "Covered 911 Service Providers," as defined above, without exception. We also decline to create a specific waiver procedure for entities to seek exemption from the rules. While we acknowledge that small or rural service providers may have limited resources or operate in remote areas, we decline to establish two tiers of 911 reliability based on economics or geography. Moreover, the rules we adopt allow flexibility for small or rural providers to comply with our rules in the manner most appropriate for their networks, and certain requirements will, by their nature, only apply to larger providers. For example, some small service providers monitor their networks directly from a central office and may not have separate NOCs; in such cases, the provider could certify that, while it does not have diverse aggregation points supplying telemetry data to diverse NOCs, it has taken reasonable alternative measures to ensure that the monitoring network in its central office is diverse.

41. Although one commenter suggests that the rules should extend further to PSAPs,[94] that question is beyond the scope of the *NPRM* in this proceeding. In any event, the record in this proceeding and our experience as set forth in the *Derecho Report* does not reflect avoidable failures on the part of PSAPs, but rather on the part of their service providers. We therefore disagree that Commission action should primarily "touch[] on the benefits to PSAPs of working with network providers to purchase diverse and redundant services where available."[95] Moreover, there are significant questions of

[89] American Cable Association Comments at 6.

[90] *See* Mission Critical Partners Comments at 3 (arguing that rules should apply to backhaul providers and aggregators of 911 call traffic).

[91] *Compare* APCO Comments at 2 (arguing that data centers and other facilities that host NG911911 capabilities "should also be subject to best practices and the Commission's rules, at least to the extent permitted by relevant law") *with* Mission Critical Partners Comments at 5 ("The Commission should defer the responsibility for ESInet datacenter standards development to industry associations such as [NENA].").

[92] *See* Alaska Communications Systems Comments at 4 ("The Commission should broaden its view to include PSAPs, consumers, and other parties that contribute to the effectiveness and reliability of 911 services.").

[93] *See, e.g.*, Western Telecommunication Alliance Comments at ii ("The Commission's proposed new 911 service requirements and reporting rules are devised primarily to address potential problems of large carriers in metropolitan areas, and are largely irrelevant and even harmful to disaster recovery efforts by RLECs in their rural service areas."); Alaska Communications Systems Comments at 3 ("[I]t is not always possible to follow every industry best practice in remote areas such as the Alaska bush.").

[94] *See* Alaska Communications Systems Comments at 4 ("The Commission should broaden its view to include PSAPs, consumers, and other parties that contribute to the effectiveness and reliability of 911 services.").

[95] *Id.* at 4-5.

federalism involved in regulation of local government entities, and a strong consensus among commenters that the Commission should not interfere with the internal operations of PSAPs.[96] While we agree that each of these groups plays a role in 911 reliability and encourage PSAPs to contract for the highest level of service available, we conclude that a regulatory focus on entities that provide 911 capabilities to PSAPs is most consistent with the Commission's objectives in this proceeding, based on the findings of the *Derecho Report*, our prior experience, and the comments in the record as set forth above. Moreover, in light of the limited focus of this proceeding, we do not believe it is necessary to determine whether to classify all entities or networks directly or indirectly involved with 911 calls to a PSAP as "telecommunications," as the Pennsylvania PUC suggests.[97] Because the term "telecommunications" has a specific meaning under the Communications Act,[98] we seek to avoid unintended consequences of classifying a broad range of entities that provide 911 capabilities as "telecommunications."

42. As multiple commenters observe, the Commission's approach to 911 reliability must support and encourage the development of new technologies while ensuring that legacy infrastructure remains reliable as long as it is in use.[99] We must not inadvertently discourage innovation by assuming that future 911 capabilities will require the same level of oversight as those in place today.[100] Therefore, while we strongly support the transition to NG911,[101] 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.[102] We may, however, revisit this distinction in the future as technology evolves, as discussed below with regard to review and sunset of the rules.

43. Similarly, we decline at this time to cover all operators of emergency services Internet protocol networks (ESInets), as proposed in the *NPRM*.[103] Some ESInets may provide capabilities other than those at issue here, and other ESInets may be operated directly by PSAPs and 911 authorities. Under the rules we adopt today, ESInet operators will be required to certify reliability only to the extent they qualify as Covered 911 Service Providers under our rules.

[96] One commenter notes that the Commission has supported CSRIC's development of best practices applicable to PSAPs and consumers, underscoring the "interdependence of network providers, PSAPs, and consumers in ensuring effective and reliable 911 services." *See* Alaska Communications Systems Comments at 5-6 (citing CSRIC III Working Group 8, E911 Best Practices Final Report, Part 1 at 7, Part 2 at 20).

[97] *See* Pennsylvania PUC Comments at 3-4.

[98] *See* 47 U.S.C. § 153(50).

[99] *See, e.g.*, Fairfax County Comments at 11 ("Ultimately the deployment of Next Generation 911 is the best approach to improving 911 redundancy and reliability, but interim improvements are needed in the meantime."); NATOA Comments at 3 ("While we welcome the opportunities that new technologies bring to public safety communications capabilities, we emphasize that as new technologies evolve, the reliability of the legacy network remains a critical asset in stable emergency communications.").

[100] *See* NENA Comments at 14 (noting generally that "NG911 systems will require somewhat different reliability rules").

[101] *See* RECOMMENDATIONS FOR NEXT GENERATION 911 LEGAL FRAMEWORK: FCC REPORT TO CONGRESS (2013) (submitted pursuant to § 6509 of the Next Generation 911 Advancement Act of 2012, enacted as part of the Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96, tit. VI, subtitle E)

[102] SMS-based text-to-911 capabilities, for example, are not functionally equivalent to the core 911 capabilities described above (*i.e.*, call routing and number/location information) and therefore fall outside the scope of this *Report and Order*.

[103] *See 911 Reliability NPRM*, 28 FCC Rcd at 3425 ¶ 23.

C. Implementation Approach

44. The *911 Reliability NPRM* proposed four alternative options for implementation of recommendations in the *Derecho Report*: (1) reporting, (2) certification, (3) reliability requirements, and (4) site inspections or compliance reviews.[104] It noted that the implementation options need not be mutually exclusive, and sought comment "on whether each of these approaches can stand alone, or whether the Commission should adopt two or more options as part of an integrated approach."[105] The *NPRM* also posed a variety of questions regarding records retention and documentation of compliance with best practices or reliability requirements. As discussed below, we adopt rules to require that Covered 911 Service Providers (1) take reasonable measures to ensure reliable 911 service and (2) certify annually that they do so by adhering either to specified, essential practices based on established industry consensus or to appropriate alternative measures demonstrated to be reasonably sufficient to mitigate the risk of failure.

1. Reasonable 911 Reliability Measures Required

45. To promote reliable 911 service, we adopt a rule that requires all Covered 911 Service Providers to take reasonable measures to ensure 911 circuit diversity, availability of backup power at central offices that directly serve PSAPs, and diversity of network monitoring links (the "reasonable measures" requirement). As commenters point out, reasonable measures may vary to some degree by location, service provider, and technology.[106] The record demonstrates, however, a number of concrete and objective indications of whether a service provider's practices with respect to 911 reliability are reasonable.

46. In particular, best practices are developed in a "consensus-based environment"[107] reflecting the collective judgment of industry, government, and other stakeholders. It follows that compliance with best practices is a strong indication that a service provider is taking reasonable measures to ensure reliable 911 service. While there may be situations in which it would be reasonable for a service provider to depart from best practices,[108] there should be a reasonable basis for such decisions, coupled with appropriate steps to compensate for any increased risk of failure. Thus, where service providers employ alternative measures in lieu of best practices, they should be able to explain why those measures are appropriate and reflect reasonable measures to provide reliable 911 service.

47. The certification process we adopt today is founded in industry best practices and will provide the Commission with important information on the reliability of 911 services nationwide. It will also provide Covered 911 Service Providers with flexibility and a means of demonstrating that they are taking reasonable measures to ensure the reliability of their 911 service. Below, we provide additional guidance on what constitutes reasonable measures for the purposes of these rules.

2. Annual Reliability Certification

48. Under the rules we adopt today, Covered 911 Service Providers will be able to demonstrate that they are taking reasonable measures to provide reliable 911 service through the annual certification process discussed below. A Covered 911 Service Provider that performs all the specific certification elements outlined in our rules regarding 911 circuit auditing, backup power at central offices that directly serve PSAPs, and diverse network monitoring links, may certify that it has so performed these elements without providing additional documentation to support its certification that it has met the

[104] *Id.* at 3425-29 ¶¶ 24-31.

[105] *Id.* at 3425 ¶ 24.

[106] *See, e.g.*, Alaska Communications Systems Comments at 6 (arguing that "[a]ny additional Commission compliance rules should allow for flexibility to adapt to local and regional conditions").

[107] ATIS Comments at 6.

[108] *See id.* at 5-6.

reasonable measures requirement.[109] The Covered 911 Service Provider's certification that it has performed all these elements will be deemed to satisfy the obligation to take reasonable measures to provide reliable 911 service, provided that the certification is accurate and complete.[110] In the alternative, if a Covered 911 Service Provider cannot certify affirmatively to every element in a substantive area, but believes that its actions are nevertheless reasonably sufficient to mitigate the risk of 911 service failure based on the configuration of its network and other factors, then it may certify that it has taken alternative measures in that substantive area.[111] For each element where the Covered 911 Service Provider certifies to taking alternative measures, it must include with its certification a brief explanation of those alternative measures with respect to each PSAP, central office, or 911 service area where they are in use, and why those measures are reasonable under the circumstances to mitigate the risk of failure.[112] Finally, a Covered 911 Service Provider may respond that certain elements of the certification do not apply to all or part of its network, but it must include with its certification a reasonable explanation of why those elements are not applicable.

49. We require Covered 911 Service Providers to maintain for two years the records supporting each annual certification and to make relevant records available to the Commission upon request.[113] For providers with existing electronic recordkeeping capabilities, these records must be maintained in an electronic format for ease of access and review. While certifications require only a brief description of alternative measures, we reserve the right to request additional information, at the time of certification or thereafter, to verify the accuracy of a certification or determine whether alternative measures are reasonable. This approach lessens the reporting burden on service providers while ensuring that supporting documentation is available when necessary. Examples of such records include diagrams of network routing, records of circuit audits, backup power deployment and maintenance records, and documentation of network monitoring routes and capabilities.

50. The *911 Reliability NPRM* observed that the certification approach "could help ensure that senior management is aware of significant vulnerabilities in the 911 network and accountable for its decisions regarding design, maintenance, and disaster preparedness."[114] It also inquired whether existing Commission certification schemes, or those under other statutes, provide a model for addressing 911 reliability.[115] For example, under the Commission's Consumer Proprietary Network Information (CPNI)

[109] We note, however, that all Covered 911 Service Providers must maintain for two years records to substantiate their certifications. *See* ¶ 49, *infra*.

[110] The Commission reserves the right to review affirmative certifications and to request additional information to verify whether a Covered 911 Service Provider has, in fact, performed all certification elements. If a Covered 911 Service Provider cannot substantiate its certification responses, it will not be deemed to be taking reasonable measures to provide reliable 911 service and may be subject to enforcement action. *See* ¶ 49, *infra*.

[111] As noted below, all Covered 911 Service Providers must audit and tag critical 911 circuits and audit network monitoring links and aggregation points, but they may choose to take reasonable alternative measures in lieu of eliminating single points of failure based on the results of those required audits.

[112] If a provider discovers, during the course of completing the work necessary for this certification, that it has an issue which it cannot remediate prior to certification, it may certify that it has identified the issue and is in the process of taking appropriate steps to address the issue. Its certification should include a description of the steps it is taking, the date by which it anticipates such remediation will be completed, and why it believes such steps are sufficient to mitigate the risk of failure. As with certifications based on alternative measures, explanations of ongoing remediation will be subject to further review by the Bureau. *See* ¶¶ 62-63, *infra*.

[113] When the Commission is inquiring into a certification submitted pursuant to Part 12 of the Commission's rules, Covered 911 Service Providers should continue to retain all records relevant to the inquiry, even if the records pertain to events that occurred more than two years before.

[114] *911 Reliability NPRM* 28 FCC Rcd at 3427 ¶ 28.

[115] *Id.* at 3427-28 ¶ 29.

certification model, an officer of the telecommunications provider acting as its agent must sign and file a certification including a statement that the officer has "personal knowledge" that the company has established operating procedures that adequately ensure compliance with the CPNI rules.[116] Similarly, under the Commission's Equal Employment Opportunity (EEO) certification model, multichannel video programming distributors (MVPDs) must certify their employment practices by filing Form 396-C, which requires a company official to state whether the MVPD's operating procedures ensure compliance (or non-compliance) with the EEO requirements.[117] If the official answers in the negative, then that official must attach an explanation.

51. The record here reflects broad support for a certification approach, although commenters disagree about what certification might entail. Verizon, for example, states that "[t]he most effective approach would be for the Commission to collaborate with industry and other stakeholders to create an annual certification program," but adds that "[i]f the provider is not complying with a particular practice, the provider could explain in the report why not and, if applicable, describe the actions it is taking that would mitigate the relevant risk the practice is intended to address."[118] Frontier states that while "the current record demonstrates that additional Commission mandates are unwarranted, if the Commission were to take further steps in this area, the consensus amongst a majority of commenters is that a certification process is the most appropriate method."[119] While Frontier favors the current system of voluntary best practices above any form of regulation, it notes that "the certification system is preferable over the other proposed implementation options because it is the most efficient use of resources."[120] Similarly, AT&T states that "[t]o the extent the Commission proceeds with regulation in the area of 911 circuit auditing, it should require 911 Service Providers to certify annually that they are conducting computerized diversity audits consistent with industry best practices," and adds that "[s]uch a requirement would be an appropriate, incremental step to reassure the Commission that providers adhere to best practices to bolster network reliability and resiliency."[121]

52. Other commenters support certification requirements in part, but argue that they should be accompanied by other measures. The California Public Utilities Commission (California PUC), for example, "recommends that the FCC adopt a certification scheme, in combination with minimum backup power requirements" and an additional reporting requirement that would "provide States with timely access to the state-specific data pertaining to 911 networks."[122] Fairfax County recommends that network operators be required to certify the result of circuit audits to the Commission, but adds that "at a more fundamental level, network operators and service providers should be required to maintain a minimum specified level of physical diversity for their 911 circuits."[123]

53. Alaska Communications Systems, by contrast, states that "[the] industry best practices . . . must be evaluated and implemented by individual service providers within the context of the specific needs and resources available to serve specific PSAPs," and adds that, "for this reason, the Commission's proposal to require periodic compliance certifications from service providers is flawed."[124] We disagree

[116] *See* 47 C.F.R. § 64.2009.

[117] *See* 47 U.S.C. § 554; 47 C.F.R. § 76.75(b); Commission Form 396, *available at* http://transition.fcc.gov/Forms/Form396/396.pdf.

[118] Verizon Comments at 7, 14.

[119] Frontier Reply Comments at 3.

[120] Frontier Comments at 6.

[121] AT&T Comments at 13-14.

[122] California PUC Comments at 4-5.

[123] Fairfax County Comments at 5.

[124] Alaska Communications Systems Comments at 7.

that requiring certification to ensure the reliability of 911 service will stifle the development of best practices, generally, and with respect to issues affecting 911 service, specifically. The elements of the certification process we adopt today are designed to implement best practices already established through industry consensus that have proven most relevant to reliable 911 service. We conclude that the additional detail in our rules is warranted to ensure a reliable and robust 911 network based on our experience – specifically, the analysis of NORS and DIRS data over the past eight years.

54. While we agree with the broad range of commenters who favor a certification approach, we conclude that a very high-level certification will not provide the Commission with either the information it needs to identify important weaknesses in 911 networks or a reasonable basis on which to hold service providers accountable for decisions affecting 911 reliability. We recognize also that a far-reaching certification requirement could impose a heavy burden on providers that have been complying with critical best practices. Therefore, we require all Covered 911 Service Providers to certify annually to certain basic measures in the three substantive areas, and delegate to the Bureau the responsibility to review the certifications and take additional action as appropriate. We also delegate to the Bureau the authority and responsibility to develop the certification form and filing system.

55. As with certifications and applications filed with the Commission, the reliability certifications will be subject to penalties for false or misleading statements both under the United States Code[125] and the Commission's rules.[126] The certification shall also be accompanied by a statement explaining the basis for such certification[127] and shall be subscribed to as true under penalty of perjury in substantially the form set forth in Section 1.16 of the Rules.[128]

56. *Certification Standards.* Some commenters call for the creation of a process to define and/or maintain the certification standards and procedures.[129] CenturyLink suggests that a "working group of interested public and private stakeholders should be charged to review best practices and other proposals to determine whether a core subset of them should be adopted."[130] Likewise, Verizon suggests that the Commission convene a group of experts to identify a core set of standards that could be used as the basis for certifications.[131] Other commenters would similarly turn to multi-stakeholder bodies like CSRIC in search of a solution.[132] The process that these commenters describe, however, is virtually indistinguishable from our existing CSRIC process. In fact, CSRIC III was asked to "review the existing CSRIC/NRIC 911 best practices and recommend ways to improve them, accounting for the passage of time, technology changes, operational factors, and other identified gaps."[133] These revised best practices are available to stakeholders for application on a voluntary basis.[134] Thus, we see no reason to defer our

[125] *See* 18 U.S.C. § 1001 (false statements to the federal government).

[126] *See* 47 C.F.R. § 1.17 (truthful and accurate statements to the Commission).

[127] Specifically, the rules require each Certifying Official to attest that the Covered 911 Service Provider has adequate internal controls to bring material information to his or her attention, and that the Certifying Official reasonably believes that he or she is aware of all material information necessary to complete the certification. *See* App. B, *infra*.

[128] *See* 47 C.F.R. § 1.16 (unsworn declarations under penalty of perjury).

[129] *See* Pennsylvania PUC Comments at 13; Fairfax County Comments at 5.

[130] *See id.* at 5.

[131] *See* Verizon Comments at 8.

[132] *See* NTCA Comments at 3 ("The Commission should install a certification scheme using applicable industry-defined best practices as established through CSRIC.").

[133] *See* CSRIC III, Working Group 8, E911 Best Practices Final Report – Part 2 at 3 (March 2013), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRICIII_6-6-12_WG8-Final-Report_Pt2.pdf.

[134] *See id.* at 10, App. 3-4.

refinement and implementation of these best practices in a Commission rule, in light of our experiences with voluntary standards set forth above.

57. Others note that CSRIC best practices may be vague or insufficient to suit the purpose at hand.[135] While we agree that best practices may not always provide exhaustive guidance in every situation, we note that many service providers have realized significant improvements in network reliability through their thorough and consistent implementation.[136] We also observe that the certification elements we adopt are consistent with relevant CSRIC best practices, with additional refinements based on sound engineering practices in the 911 context. This approach provides more specific guidance to the industry while assuring the public safety community that our rules fill any gaps in existing best practices with measurable standards for certification.

58. Finally, some commenters point out that the deployment of NG911 might have an impact on the certification standards.[137] We understand that, as NG911 deployment advances, our certification standards may have to change, and we may need to turn to multi-stakeholder bodies like CSRIC in the future for recommendations in these areas. Accordingly, we adopt certification standards that are consistent with current best practices but also flexible enough to account for differences in 911 and NG911 networks.

59. *Certifying Official.* To ensure accuracy and accountability, each certification must be made by a corporate officer responsible for network operations in all relevant service areas. Thus, the certifying official must have supervisory and budgetary authority over a Covered 911 Service Provider's entire 911 network, not merely certain regions or service areas.

60. Some commenters argue that service providers should have flexibility to execute the certification at a lower level in the company. AT&T, for example, suggests that company directors should be permitted to execute the certification as they "are better-positioned than officers to personally attest to the adequacy of a company's local auditing procedures."[138] As AT&T recognizes, however, our CPNI rules require compliance certification by an officer with personal knowledge.[139] Here, too, we do not believe that certification by personnel without supervisory and/or budgetary authority over network operations would hold management accountable for decisions affecting 911 reliability or create the same incentive for service providers to make 911 infrastructure a priority at the corporate level, particularly since these investments typically depend on budgeting decisions over which only officers would have decisive authority. To that end, the certification must also reflect the existence of internal controls sufficient to ensure that the certifying official has received all material information necessary to complete the certification accurately.

61. *Effect of Certification.* Under the certification process we adopt, a Covered 911 Service Provider that performs all the certification elements in a substantive area is deemed in compliance with our rules requiring reasonable measures in that area. This result is subject only to any determination we

[135] *See* Fairfax County Comments at 5 (commenting that the CSRIC best practice upon which we base our 911 circuit auditing requirement "provides a starting point, but additional details need to be added to this and other CSRIC best practices to provide more measureable standards for what comprises acceptable network diversity as well as an acceptable diversity audit.").

[136] *See, e.g.*, ATIS NETWORK RELIABILITY STEERING COMMITTEE, 2010-2012 OPERATIONAL REPORT at 6-15 (July 2013), *available at* https://www.atis.org/docstore/product.aspx?id=28010 (outlining recent efforts to study and make recommendations on various network reliability issues and noting that "[t]he continued efforts of NRSC member companies have directly and positively impacted the resiliency and reliability of the Nation's networks, which ultimately benefits all users").

[137] *See* CenturyLink Reply Comments at 6.

[138] *See* AT&T Comments at 14 n.12.

[139] *Id.; see* 47 C.F.R. § 64.2009(e).

may make afterward, based on complaints, outage reports or other information, that the Covered 911 Service Provider did not, in fact, perform those elements as claimed in its certification.[140] Thus, Covered 911 Service Providers that perform all the specified elements will be deemed in compliance with our rules as adopted in this *Report and Order*. We do not contemplate further Commission action under these rules in response to affirmative certifications absent some indication that such certifications were not accurate and complete.[141]

62. If, however, a Covered 911 Service Provider certifies that it has taken alternative measures to mitigate the risk of failure, or that a certification element is not applicable to its network, its certification is subject to a more detailed Bureau review. In such cases, the Covered 911 Service Provider must provide an explanation of its alternative measures and why they are reasonable under the circumstances, or why the certification element is not applicable. The Bureau will consider a number of factors in determining whether the particular alternative measures are reasonably sufficient to ensure reliable 911 service. Such factors may include the technical characteristics of those measures, the location and geography of the service area, the level of service ordered by the PSAP, and state and local laws (such as zoning and noise ordinances). The Bureau may rely on information from a variety of sources, including: (1) the certifications and descriptions of alternative measures, (2) supplemental responses to Commission inquiries, (3) supporting records retained pursuant to the record retention requirement, (4) NORS and DIRS data, (5) formal and informal complaints, and/or (6) news reports or other information available to the Commission. We provide further guidance regarding reasonably sufficient alternative measures in each substantive certification area below in section III.D.

63. If the Bureau's review indicates that a provider's alternative measures are not reasonably sufficient to ensure reliable 911 service, the Bureau should engage with the provider and other interested stakeholders (*e.g.*, affected PSAPs) to address any shortcomings. To the extent that a collaborative process with a provider does not yield satisfactory results, the Bureau may order remedial action, consistent with the authority delegated in this *Report and Order*. For example, if a Covered 911 Service Provider does not certify that it has performed a given certification element and has not adopted reasonably sufficient alternative measures to compensate for the increased risk of failure, the Bureau should work with the provider to eliminate avoidable single points of failure, to install additional backup power capabilities at a central office that directly serves a PSAP, or to upgrade its network monitoring facilities; in situations where collaborating with the provider does not yield satisfactory results, the Bureau may order the provider to take remedial action. Any service provider ordered to take remedial action may seek reconsideration or review of the Bureau's decision in accordance with the Commission's rules.[142] In extreme cases, such as where a provider is not acting in good faith, the Bureau may also refer cases where alternative measures are deemed unreasonable to the Enforcement Bureau for further action as appropriate. This approach will place the least burden on those Covered 911 Service Providers that provide consistently reliable 911 service, while allowing the Commission to focus its attention and resources where most needed.[143]

64. *Certification Phase-In.* The rules we adopt today, including the underlying obligation to take reasonable measures to provide reliable 911 service, become effective thirty days after publication in the Federal Register. Although information collection requirements pursuant to those rules will not become effective until approval by the Office of Management and Budget (OMB) pursuant to the

[140] We note that possible violations of our rules may be referred to the Enforcement Bureau for further action as appropriate.

[141] Of course, all Covered 911 Service Providers remain subject to the Commission's more general authority under Titles II and III of the Communications Act and the remedies under that Act.

[142] *See generally* 47 C.F.R. §§ 1.101-1.117.

[143] *See* Blooston Rural Carriers Comments at 2-5; Western Telecommunications Alliance Comments at 3-4; AT&T Comments at 3.

Paperwork Reduction Act,[144] the substantive obligation to take such reasonable measures is not contingent on such approval. Because certain certification elements (*e.g.*, circuit diversity audits) require time for implementation, the first full certification will be due *two years* from the effective date of the substantive rule requiring service providers to undertake such reasonable measures.[145]

65. Although service providers indicate that they already perform many of the elements of our annual certification, the rules we adopt will require a phase-in period so that all covered entities, particularly smaller entities with limited staff and resources, have time to come into full compliance. Therefore, we require that, one year after the effective date of the rules, all Covered 911 Service Providers file an initial certification that they have made substantial progress toward meeting the standard of the full certification. To allow service providers time to implement the best practices reflected in the certification, we define "substantial progress" as at least 50-percent compliance with each of the three substantive certification requirements.[146] We delegate to the Bureau authority to implement this initial certification, including the form and process through which it is submitted, consistent with the principles of substantial progress described above. After the first full certification two years from the effective date of the rules, all Covered 911 Service Providers will file a 911 reliability certification on an annual basis.

3. Implementation Approaches Not Adopted

66. *Reporting.* Under one approach proposed in the *911 Reliability NPRM*, 911 service providers would be required to periodically file reports on their compliance with best practices, which might provide both the Commission and industry with greater knowledge of the state of 911 infrastructure. However, such an approach would not require service providers to address noncompliance with such best practices that may lead to vulnerabilities in their networks. Public-safety commenters generally view reporting as an incomplete solution, while service providers oppose it as unnecessarily burdensome.[147] APCO, for example, supports periodic reporting by service providers as a "partial solution" but adds that "[e]qually important, the Commission will need to review carefully those reports in a timely manner and seek further information and clarification when the reports are incomplete or reflect deficiencies."[148]

67. We are not convinced that a reporting approach would produce adequate assurance of actual compliance with best practices and associated improvements in 911 reliability to outweigh any costs of complying with reporting requirements. As noted in the *NPRM*, and confirmed by Verizon, our experience with the one-time reports required by section 12.3 of our rules did not appear to result in a "material benefit that outweighed its costs."[149] To the extent that reporting could provide additional data on 911 reliability, we note that the specific information directly related to best practices critical to 911 service reliability will more likely be revealed through the certification process we adopt today. Moreover, the approach we adopt *lessens* the reporting burden on service providers whose certifications indicate that they already are taking reasonable measures to ensure reliable 911 service, while providing the Commission with a more effective enforcement mechanism where certification or subsequent performance reveals a need for corrective action.

---

[144] 44 U.S.C. §§ 3501 *et seq.*

[145] As noted above, the information collection and recordkeeping procedures we adopt today in connection with both the Initial and Annual Reliability Certifications will become effective upon OMB approval.

[146] For example, regarding circuit diversity, Covered 911 Service Providers must certify they have conducted at least 50 percent of the circuit audits described more fully in Section D.1 below.

[147] *See id.* at 7 (arguing that "resources are best directed at improving reliability and resiliency in the network – not completing paperwork").

[148] APCO Comments at 2.

[149] Verizon Comments at 12-13; *911 Reliability NPRM*, 28 FCC Rcd at 3426-27 ¶ 27.

68. *Reliability Requirements.* Under this approach, the Commission would adopt rules setting mandatory standards for the design and operation of 911 networks in key areas identified in the *NPRM*. This approach has the advantage of ensuring that service providers adhere to mandatory network reliability standards, but it may be unduly prescriptive and may not sufficiently account for changing technologies and legitimate differences in network design.[150] Commenters also express concern that the Commission could risk inadvertently discouraging innovation by adopting rules based on legacy technologies rather than promoting deployment of more reliable NG911 services.[151] Although we conclude that Commission action is warranted on a nationwide basis, we recognize that a "one-size-fits-all" approach may be infeasible and that, for a variety of reasons, service providers may opt to achieve a reasonable level of 911 reliability through other means than those specifically stated in existing best practices. The certification approach we adopt is more flexible than uniform standards and will allow service providers to implement best practices in the manner most appropriate for their networks and service areas. Without imposing inflexible reliability requirements, our certification approach also offers reasonable assurance to PSAPs and the public that known vulnerabilities in 911 networks will be identified and corrected promptly.

69. *Site Inspections and Compliance Reviews.* Although some commenters argue that inspections and reviews would ensure a high level of compliance with best practices,[152] others contend that they could place significant administrative burdens both on the Commission and on service providers and would yield little benefit for the cost incurred.[153] Verizon, for example, comments that "recordkeeping for its own sake will not help 911 resiliency," and that "[t]he Commission should avoid any prescriptive rules that would require 911 service providers to make specific improvements or adopt certain practices and open their facilities for Commission-led periodic site inspections."[154] The Pennsylvania PUC, by contrast, notes its support for "testing, maintenance, and record keeping requirements" with respect to central-office backup power.[155]

70. Given the less burdensome options available and the Commission resources that would be required to perform site inspections, we are not persuaded that the benefits of this approach would outweigh the costs. We believe that the more appropriate course would be to rely on inspections and compliance reviews only in those individual cases where the certification or subsequent performance raises significant questions about the provider's compliance with our rule designed to ensure 911 service reliability. Accordingly, we would anticipate seeking additional information only when necessary to determine whether a certification is complete and accurate or, in the case of certifications based on alternative measures, when necessary to assess whether such alternative measures are reasonably sufficient to minimize the risk of failure. Moreover, by requiring retention and production of such records upon request, our certification approach ensures accountability in cases where a certification or outage report raises concerns about a service provider's 911 network, while avoiding the burdens of site inspections and compliance reviews when they are not shown to be necessary.

71. *Risk-Based Approach.* NENA recommends that we adopt a "risk-based approach" of setting multiple levels of certification standards according to the relative criticality of particular network

[150] *See* CenturyLink Reply Comments at 2; Verizon Comments at 16; Telecommunications Industry Association Comments at 8; NTCA Comments at 2; AT&T Comments at 2.

[151] *See* CenturyLink Reply Comments at 6; Telecommunications Industry Association Comments at 5-6.

[152] *See* APCO Comments at 3 (supporting "the use of periodic compliance reviews and inspections of service provider facilities to verify adherence to certain standards").

[153] *See* AT&T Comments at 15.

[154] Verizon Comments at 12, 16.

[155] Pennsylvania PUC Comments at 14.

elements.[156] Under this approach, "the Commission could require carriers and [system service providers] to conduct and periodically update formal, all-hazards risk assessments for 911 special facilities and other network elements or systems related to provisioning 911 service."[157] NENA further suggests that the Commission could establish "normal" and "minimum" performance standards that would apply in individual circumstances based on the results of these risk assessments.[158] Although we agree that some form of risk assessment should play a role in service providers' allocation of resources, we have concerns that a risk-based approach to certification could be difficult to implement and enforce, especially if it requires us to supplement CSRIC best practices in order to establish multiple tiers of reliability standards. While this approach would help to ensure that compliance costs would be matched to some objective measure of risk, the periodic risk assessments that NENA describes could be complex and burdensome on a national scale and would likely retain some subjectivity due to varying priorities and tolerances for risk among service providers. We believe that it is preferable to rely upon the best practices already established through consensus as the appropriate benchmark for our rules, at least in the first instance and until we gain more experience.

72. Furthermore, NENA suggests that risk assessments could help differentiate between investments needed in "sparsely-populated or low-risk communities" as opposed to "densely-populated or high-risk communities."[159] We decline to adopt rules that, even if unintentionally, could discourage needed investments in 911 infrastructure serving rural and remote areas. The certification approach we adopt holds all Covered 911 Service Providers to a single standard with flexibility to allocate resources based on risk, service area, and any other relevant factors, as long as they employ measures reasonably sufficient to mitigate the risk of failure.

4. Costs and Benefits of Commission Action

73. Reliable 911 service provides public safety benefits that, while sometimes difficult to quantify, are enormously valuable to individual callers and to the nation as a whole. As one commenter observes, "911 is the lifeline for safety and security for citizens and is seen by both citizens and all levels of government as a part of the critical infrastructure that supports public safety."[160] As noted above, these benefits are reflected in our statutory mandate to promote the safety of life and property.[161] The *911 Reliability NPRM* further noted that "the ability to call 911 during a disaster, medical emergency or other time of need may literally make the difference between life and death."[162] Accordingly, the *NPRM* sought to quantify the potential benefits of improvements in 911 reliability through the "valuation of a statistical life" (VSL) employed by the U.S. Department of Transportation (DOT). At the time we issued our

[156] *See* NENA Comments at 4.

[157] *Id.*

[158] *See id.* at 5.

[159] *Id.*

[160] VIRGINIA SECURE COMMONWEALTH PANEL, E911 SUB-PANEL, THE STATE OF E911 IN VIRGINIA at 3 (May 6, 2013), *available at* http://apps.fcc.gov/ecfs/document/view?id=7022312861.

[161] *See* 47 U.S.C. § 151.

[162] *911 Reliability NPRM*, 28 FCC Rcd at 3424 ¶ 22.

NPRM, DOT estimated this value at $6.2 million.[163] Since then, the agency has increased that estimate to $9.1 million in current dollars.[164]

74. The *NPRM* also cited a 2002 study of 911 calls in Pennsylvania that found that, when E911 location information was provided contemporaneously with a 911 call, response time was notably shortened and correlated with a 34-percent reduction in mortality rates from cardiac arrest within the first 48 hours following the incident.[165] Based on this data, the *NPRM* estimated that "[t]he study's Pennsylvania results, if representative of all states, would imply there are 341,000 cardiac incidents nationwide each year and a saving of 4,142 lives per year nationwide" through the reduction in mortality risk attributable to E911 location capabilities.[166]

75. The conclusions of the Pennsylvania study provide a basis for a rough estimate of the benefits of increasing 911 reliability. The *NPRM* estimated that "if storms cause as much as 1.25 percent of the nation's population to have such delayed access to 911 for one week each year, the expected annual saving would be at least one life."[167] We cannot, of course, predict with any certainty the likelihood of catastrophic emergency events. But we conclude for several reasons that the total benefit of the rules we adopt today will far exceed the $9.1 million base value of one statistical life. For one thing, the Pennsylvania Study captured only the lives lost when ambulances are delayed due to less accurate location information. It therefore failed to capture lives that could be lost if ambulances do not arrive *at all* due to a lack of reliable access to 911, a problem our rules are intended to address. Furthermore, our floor value considers only the benefits attributable to cardiac emergency calls, which, according to the Pennsylvania Study, accounted for less than 20 percent of medical emergency calls and less than 10 percent of total emergency calls.[168] Our estimated benefit of saving at least one life per year, therefore, likely *underestimates* the expected benefits from 10 percent of 911 calls and fully excludes *all* of the expected benefits from the remaining 90 percent of 911 calls, which involve a broad range of risks to safety of life and property beyond the cardiac emergencies examined in the Pennsylvania Study.

76. No commenter questions the basic premise that 911 communications provide significant public health and safety benefits. Nor has any commenter provided an alternative method of quantifying the public safety benefits associated with reliable 911 service. However, several commenters argue that the Pennsylvania Study focused on E911 location information rather than 911 reliability during disasters, and therefore is not applicable in this proceeding as a measure of the life-saving benefit of reliable 911

---

[163] *See* Memorandum from Polly Trottenberg, Assistant Secretary for Transportation Policy, U.S. Dep't of Transp. and Robert S. Rivkin, General Counsel, U.S. Dep't of Transp., to Secretarial Officers and Modal Administrators, U.S. Dep't of Transp., Treatment of the Economic Value of a Statistical Life in Departmental Analysis - 2011 Interim Adjustment (July 29, 2011) (DOT Statistical Life Valuation).

[164] *See* Memorandum from Polly Trottenberg, Under Secretary for Policy, U.S. Dep't of Transp. and Robert S. Rivkin, General Counsel, U.S. Dep't of Transp., to Secretarial Officers and Modal Administrators, Guidance on the Treatment of the Economic Value of a Statistical Life (VSL) in U.S. Department of Transportation Analyses (February 28, 2013), *available at* http://www.dot.gov/sites/dot.dev/files/docs/VSL%20Guidance%202013.pdf.

[165] *See* SUSAN ATHEY & SCOTT STERN, THE IMPACT OF INFORMATION TECHNOLOGY ON EMERGENCY HEALTH CARE OUTCOMES, Jan. 2002, *available at* http://kuznets.fas.harvard.edu/~athey/itemer.pdf (Pennsylvania Study).

[166] *911 Reliability NPRM*, 28 FCC Rcd at 3433 ¶ 43 n.100.

[167] *Id.* We also note that our estimate of 341,000 cardiac incidents being reported nationwide to 911 is roughly one-fourth of the estimated coronary attacks occurring each year in the United States. The American Heart Association estimates that each year 785,000 Americans have a new coronary attack and 470,000 have a recurrent attack. These figures, which sum to 1.255 million cardiac incidents, suggest that our estimate of 341,000 is very conservative or, if it is accurate, that only 27 percent of such incidents are called in to 911. *See* Heart Disease and Stroke Statistics - 2012 Update: A Report from the American Heart Association at 4, *Circulation* (Dec. 15, 2011), *available at* http://circ.ahajournals.org/content/125/1/e2.full.pdf+html.

[168] *See* Pennsylvania Study, *supra* note 165, at 31.

service.[169] If, however, the delivery of E911 location information has been linked to a notable reduction in mortality risk, as the Pennsylvania Study suggests, a loss of location information necessary for such service – not to mention a complete loss of 911 service – would produce a corresponding *increase* in mortality risk. We therefore conclude that our $9.1 million floor value for the requirements' expected benefit is a very conservative estimate, and that the total benefit to the safety of life and property will be considerably higher.

77. Even if the *NPRM* "fails to identify any specific harm to an individual—much less a death or serious injury—caused as a result of a failure to reach emergency services promptly during the derecho,"[170] as AT&T asserts, we consider it fortunate that the effects of the derecho were not worse given the serious problems it revealed. Moreover, one large PSAP alone did not receive nearly 1,900 calls to 911 during the derecho, suggesting that numerous callers were, in fact, deprived of access to vital emergency services.[171] Thus, whether we calculate mortality risk based on location information or some other component of 911 service, and regardless of the precise statistical value we assign to each human life, the record reflects a quantifiable risk of harm to public safety through the absence or failure of 911 capabilities and corresponding benefits to public safety through improved 911 reliability. No commenter seriously disputes that reliable 911 service saves lives and minimizes the impact of additional hazards to the safety of our citizens and their homes and other property.

78. The *911 Reliability NPRM* estimated total costs to service providers of $16.1 million to $44.1 million.[172] By relaxing or eliminating several of the requirements proposed in the *NPRM*, however, we have reduced the impact on service providers far below those estimates, and within an acceptable range of the $9.1 million floor value of benefits estimated in this *Report and Order*. As explained below, we estimate that the total annual incremental cost to service providers is approximately $9 million, which includes $6.4 million for circuit audit costs, $1.9 million for backup power costs, and $732,000 for monitoring costs.[173] We address the estimated costs of each certification element in more detail below in section III.D.

79. Some commenters, particularly 911 service providers, argue that the cost benefit-analysis in our *NPRM* overstates the expected benefits[174] and underestimates the costs of implementing the certification requirements we adopt today.[175] As noted below, however, by limiting the scope and nature of our requirements, we believe that we have reduced the potential costs associated with them.[176] We find

[169] *See* AT&T Comments at 26 (arguing that the Pennsylvania Study "does not apply here").

[170] *Id.* at 25. *But see* Sullivan, Patricia, *Help Delayed For Electrocuted Man As 911 Calls Backed Up During Storm*, WASH. POST, July 19, 2012; Ruane, Michael E., *D.C. Woman Caught In The Derecho Storm Is Left Paralyzed, But Her Attitude Is Optimistic*¸ WASH. POST, Aug. 19, 2012.

[171] *See Derecho Report* at 4 (citing Fairfax County Public Notice Comments at 12).

[172] The *911 Reliability NPRM* estimated nationwide costs to all service providers of $2.2 million for circuit audits, $11.7 million to $37.5 million for backup power, and $2.2 million to $4.4 million for network monitoring, for a total of $16.1 million to $44.1 million. *See 911 Reliability NPRM*, 28 FCC Rcd at 3432-33, 3438-39, 3441 ¶¶ 41, 57, 66.

[173] *See infra*, ¶¶ 103, 130, 138.

[174] *See* AT&T Comments at 25 (arguing that the *911 Reliability NPRM* "fails to make a causal link between the regulatory remedies proposed and the asserted public interest benefits."); CenturyLink Reply at 15 ("Evidence of tangible public benefits resulting from the reliability and resiliency measures proposed in the *NPRM* is conspicuously absent.").

[175] *See* ATIS Comments at 13 ("ATIS believes that the estimated costs grossly underestimate the burden to the industry associated with the proposed recommendations."); AT&T Comments at 24 (arguing that "[t]he Commission's cost estimates are irreparably flawed"); Verizon Comments at 12 (disputing the NPRM's cost estimate for central-office backup generators); Frontier Comments at 8 (describing the "significant time and costs that are associated with auditing 911 circuits").

[176] *See infra*, Section III.D.

that our statutory mandate to promote the safety of life and property and to implement our specific statutory 911 responsibilities makes the benefits of reliable 911 service well worth these costs, particularly since the approach we adopt here is based on best practices developed through broad industry consensus. In light of the importance that the industry places on these best practices for ensuring reliability and public safety, we believe it is reasonable to conclude that the public safety benefits of encouraging service providers to implement those best practices more consistently will exceed the incremental cost of compliance.

D. Certification Requirements

1. Circuit Diversity Audits

80. Under the rules we adopt today, Covered 911 Service Providers must certify annually whether they have, within the past year, audited the physical diversity of critical 911 circuits or equivalent data paths to each PSAP they serve, tagged those circuits to minimize the risk that they will be reconfigured at some future date,[177] and eliminated all single points of failure between the selective router, ALI/ANI database, or equivalent NG911 component, and the central office serving each PSAP. In lieu of eliminating single points of failure, they may describe why these single points of failure cannot be eliminated and the specific, reasonably sufficient alternative measures they have taken to mitigate the risks associated with the lack of physical diversity. Alternatively, Covered 911 Service Providers may certify that they believe this element of the certification is not applicable to their network, although they must explain why it is not applicable. Under these rules, all Covered 911 Service Providers must conduct annual audits of the physical diversity of their critical 911 circuits and tag those circuits to prevent rearrangement, but they may take a range of corrective measures most appropriate for their networks and PSAP customers. Covered 911 Service Providers must also retain records of circuit audits for confidential review by the Commission, upon request, for two years.

81. *Critical 911 Circuits.* For purposes of the certification, "critical 911 circuits" include transmission facilities between a 911 selective router or its functional equivalent and the final point in the local exchange serving the PSAP where these facilities make an appearance (*e.g.*, the main distribution frame) before leaving this exchange on their way to the PSAP. For purposes of this requirement, a selective router is a 911 network component that selects the appropriate destination PSAP for each 911 call based on the location of the caller.[178] Critical 911 circuits also include links from ANI/ALI databases to central offices that serve PSAPs. We emphasize that we do not include in our definition of "critical 911 circuits" the connections between the calling party and the selective router that serves this person. Because IP-based NG911 networks may not employ circuit-switched technologies, we intend the auditing obligation to extend to data transport paths for the core 911 capabilities described above in Section III.B, regardless of whether they are technically "circuits."[179] Likewise, the selective router function could be hosted by a third party. The facilities connecting the third party's selective router with the PSAPs to which it is interconnected are "critical 911 circuits."

82. *Diversity.* The *911 Reliability NPRM* observed that "[i]f providers do not regularly audit the physical routes of 911 circuits and ALI links, they will be ill-equipped to verify diversity and understand, avoid, or address instances where a single failure causes loss of all E911 circuits or all ALI

[177] "Tagged" refers to an inventory management process whereby critical circuits are labeled (*e.g.*, in circuit inventory databases) to make it less likely that circuit rearrangements will compromise diversity. While we do not specify a method or technology for tagging circuits, we require service providers to take reasonable measures to prevent inadvertent rearrangement of diverse circuits over time.

[178] *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.

[179] For example, NG911 networks may use IP-based ESInets to interconnect the selective router function to the PSAP. The facilities that compose these ESInets would be considered "critical 911 circuits."

links for a PSAP."[180] It also noted that a physical diversity audit would likely have revealed vulnerabilities that led to 911 and ALI service failures to multiple PSAPs in northern Virginia during the derecho.[181] A CSRIC best practice advises network operators to "*periodically* audit the physical and logical diversity called for by network design and take appropriate measures as needed."[182] Given their importance to safety of life and property, few communications circuits could be more worthy of this treatment than the dedicated facilities that Covered 911 Service Providers use to deliver emergency calls to PSAPs. During the derecho, a number of these critical 911 circuits were clearly not provisioned with the diversity called for in the CSRIC best practice.[183] No commenter disputes that increased diversification could help prevent similar failures in the future.

83. Physical diversity, sometimes called route diversity, means that two circuits follow different routes separated by some physical distance so that a single failure such as a power outage, equipment failure, or cable cut will not result in both circuits failing.[184] Logical diversity, sometimes called equipment diversity, implies that two circuits are provisioned to use different transmission equipment, but could share the same transmission medium (for example, the same fiber or conduit). For example, two circuits that are modulated onto two wavelengths are logically diverse. If they are then placed onto two physically separate optical fibers whose routes do not meet, they are also physically diverse, provided they do not share other equipment prior to being placed on the fibers. If, instead, they are placed onto the *same* optical fiber, they are no longer physically diverse, but they retain their logical diversity. In the context of critical 911 circuits, we focus on physical diversity as the optimum standard for certification, but we also recognize that logical diversity may be appropriate where a PSAP has not ordered physically diverse service or where physical diversity is not feasible in a particular location.[185] Accordingly, we do not impose a blanket requirement that all critical 911 circuits be physically diverse in all circumstances, but we require Covered 911 Service Providers that do not provision physically diverse 911 circuits to explain why those measures are reasonably sufficient.

84. Most Covered 911 Service Providers recognize the importance of diverse 911 circuits[186] and describe rigorous procedures and high standards of care for maintaining the integrity of critical 911 circuits. AT&T, for example, notes that "[w]hen installing critical 911 circuits—such as 911 trunks to PSAPs and ALI/ANI links—AT&T follows industry best practices designed to ensure 911 network redundancy and survivability. These practices include maintaining an operational support systems inventory of all new 911 network equipment as it is deployed."[187] Frontier states that it "has a team performing diversity reviews on network elements within central offices and outside plant fibers. This

[180] *911 Reliability NPRM*, 28 FCC Rcd at 3430 ¶ 35.

[181] *Id.* at 3430 ¶ 34.

[182] *See* CSRIC Best Practice 8-7-0532, *available at* https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=8-7-0532 (emphasis added).

[183] *See Derecho Report* at 20-21.

[184] *See 911 Reliability NPRM*, 28 FCC Rcd at 3420 ¶ 13. *See also* FCC PUBLIC SAFETY AND HOMELAND SECURITY BUREAU, TECH TOPIC 14: DIVERSITY, REDUNDANCY, AND RESILIENCY - IN THAT ORDER, *available at* http://transition.fcc.gov/pshs/techtopics/techtopics14.html ("Route diversity is generally defined as the communications routing between two points over more than one geographic or physical path with no common points.")

[185] There are many variations of this deployment scenario, and CSRIC has recognized that both physical and logical diversity may be appropriate in various circumstances. CSRIC Best Practice 7-7-0532, which is used as the basis for our circuit auditing standard, states that "network operators should periodically audit the *physical and logical diversity* called for by network design and take appropriate measures as needed." (emphasis added)

[186] *See* Alaska Communications Systems Comments at 1.

[187] AT&T Comments at 11.

team performs diversity reviews of 911 circuits, and when it identifies diversity violations it notifies regional engineering; in turn the regional engineering team works to create diversity solutions."[188] In a similar vein, since the derecho, Verizon has been working directly with PSAPs to identify and make improvements to critical 911 circuit diversity throughout its footprint.[189] These and other comments lead us to conclude that most Covered 911 Service Providers now already adhere, or intend to adhere, to the circuit-auditing measures we adopt today and will incur minimal incremental costs through the certification process.[190] However, we find that the failures revealed by the derecho compel additional oversight by the Commission to ensure that vital best practices are actually followed, and continue to be followed, to bolster the reliability and resiliency of 911 networks.

85. States and public-safety commenters strongly support mandatory circuit audits,[191] or contend that service providers "should be required to maintain a minimum specified level of physical diversity for their 911 circuits."[192] Other commenters point out that the costs to perform these audits should be modest given how the circuits are typically routed in the networks of Covered 911 Service Providers.[193] The Pennsylvania PUC suggests that physical diversity requirements be imposed after an "industry-government consultation process" has developed the applicable best practices.[194]

86. Service providers, however, are mixed in their reaction to our proposal for regular audits of 911 circuit diversity. Some argue that they already have policies in place to audit and maintain circuit diversity, and that Commission mandates would be costly and inflexible. AT&T argues that imposition of regulatory obligations in the area of 911 circuit auditing, like specific physical diversity requirements, would "harm network reliability by preventing 911 Service Providers from implementing solutions tailored to the unique characteristics of their networks . . ."[195] RLECs also oppose a requirement for physical diversity on the grounds that it may not be feasible in rural areas.[196] NTCA, on the other hand, calls upon the Commission to "install a certification scheme to enable communications service providers to annually certify that 911 network services and facilities comply with applicable industry best practices as administered by CSRIC."[197] Verizon argues for the use of a collaborative group of subject matter

[188] *See* Frontier Comments at 8

[189] *See* Verizon Comments at 6.

[190] *See* ATIS Comments at 10 (arguing that mandatory circuit audits are not necessary because "communication providers do recognize the importance of maintaining 911 circuit availability and have appropriate processes in place to meet established commitments to PSAPs").

[191] *See* NENA Comments at 10; Fairfax County Comments at 3 ("Network operators/service providers should be required to conduct such audits."); City of Alexandria Comments at 5; Pennsylvania PUC Comments at 13.

[192] Fairfax County Comments at 5; City of Alexandria Comments at 4; Pennsylvania PUC Comments at 13.

[193] *See* Mission Critical Partners Comments at 6 ("Indeed we agree with the Commission that the costs associated with these audits are modest, as many of the trunks and data circuits to a single PSAP will follow similar routes. That is to say that although a PSAP may have 50 trunks, it is common that many of the trunks will follow only one or two paths and thus a commensurate number of audits is not the rule but rather the exception.").

[194] *See* Pennsylvania PUC Comments at 14.

[195] *See* AT&T Comments at 14; ATIS Comments at 10; Edison Electric Institute Comments at 7 ("Given the existence of such standards, as well as the nature of communications networks and the need for a certain level of flexibility, EEI believes that adoption by the Commission of proscriptive rules or standards is not an ideal solution to address reliability deficiencies and backup power issues.").

[196] *See* NTCA Comments at 5 ("NTCA urges the FCC to consider the unique circumstances of rural operators and refrain from implementing physical diversity requirements upon small rural carriers to the extent that they might apply to all RLEC operations."); Frontier Comments at 10; Western Telecommunications Alliance Comments at 10-11.

[197] *See* NTCA Comments at 4.

experts, like CSRIC, to define a core set of practices that would form the basis for a reliability certification.[198]

87. Assure911.net proposes a reporting scheme that would extend from 911 callers through to the PSAP that serves them.[199] As a threshold matter, we note that the circuits from the end-user to the selective router lie beyond the scope of this proceeding. AT&T also observes that reporting obligations above and beyond what would accompany the certification would require Covered 911 Service Providers to file information that "is not necessary to ensure that providers regularly carry out diversity audits."[200] Other commenters share this view.[201] We agree and decline to impose a separate reporting obligation on Covered 911 Service Providers at this time.

88. One commenter suggests that periodic failure testing of critical 911 circuits could be an alternative to the auditing approach that we adopt here.[202] We are reluctant to adopt a requirement for periodic testing of circuit failure scenarios, however, as such testing might result in short disruptions to 911 service while testing is performed. Moreover, while such an approach could help identify failed circuits, it would not necessarily reveal lapses in the diversity of functional circuits. Given these potential dangers, we conclude that this alternative would provide insufficient protection to 911 service, and to the lives and property this service is designed to protect.

89. Another commenter proposes that we consider the use of the Telecommunications Service Priority (TSP) system as a basis for circuit auditing of critical 911 circuits.[203] Mission Critical Partners argues that, among other things, the use of TSP for critical 911 circuits would help ensure prompt restoration of such circuits. TSP uses an inventory management process much like the "tagging" concept that we adopt today. Unlike tagging, however, TSP is not designed to ensure circuit diversity, which the record indicates to be of central importance in avoiding 911 failures. Rather, it is intended to hasten the circuit provisioning and restoration processes.[204] Hence, we choose not to adopt TSP as the mechanism whereby Covered 911 Service Providers manage their 911 circuit inventory.

90. *Auditing Methods.* As a number of parties have pointed out,[205] physical diversity audits need not be intrusive or disruptive. For example, the audits could be completed using a computerized examination of circuit and facility assignment data in databases. A more labor-intensive version of this process would involve human examination of circuit assignment records for critical 911 circuits. To be in conformance with the CSRIC best practice, however, an auditing method must reflect the geographic routing of circuits, as well as the logical flow of data, which could occur over a common physical path. In cases where a party provides 911 services directly to a PSAP (pursuant to contract or tariff) over leased facilities, the auditing obligation would apply to that party, and not to the facilities lessor. Although it could contract with the underlying facilities lessor, if necessary, to audit its facilities, the Covered 911 Service provider would remain responsible under our rules for ensuring compliance with the auditing requirement.

91. Although some commenters contend that "physical auditing" of 911 circuits is time-consuming and may actually damage network components that must be disassembled or otherwise

[198] *See* Verizon Comments at 13.

[199] *See* Assure911.net Comments at 3-4.

[200] *See* AT&T Comments at 14.

[201] *See* ATIS Comments at 10.

[202] *See* NENA Comments at 10.

[203] *See* Mission Critical Partners Comments at 7.

[204] *See* U.S. Department of Homeland Security, Telecommunications Service Priority, http://tsp.ncs.gov/.

[205] *See* AT&T Comments at 11-12.

disturbed in the process,[206] we believe this objection overlooks the possibility for accurate audits of records, or automated systems that perform the same function. It may be possible to conduct "highly accurate" computerized audits of physical *and* logical diversity, as AT&T asserts,[207] and such audits would satisfy the certification obligation so long as they trace the geographic routing of 911 circuits. AT&T describes one such inventory system, called the Diversity Analysis Reporting Tool (DART), which integrates logical circuit data with physical facilities data, enabling automated auditing of the diversity of critical 911 circuits.[208] AT&T further notes that "after the initial development of the tool is complete, there are minimal incremental costs to operating and maintaining DART."[209] Similarly, Verizon notes that it is "working on a means to store network information in a new inventory system to better facilitate response and restoration."[210] This system would "automate the process of grouping a PSAP's circuits, thus eliminating one of the manual steps [Verizon] take[s] today."[211] Although Verizon states that the costs of subsequent audits using this system are unclear, it acknowledges that the automated process "may require slightly less time" than previous audits.[212]

92. Other Covered 911 Service Providers, while asserting that they audit critical 911 circuits for diversity, do not use automated systems.[213] CenturyLink, for example, lacks the capability to perform computerized audits and opposes a requirement that such a method be used to conduct audits.[214] Nevertheless, even relatively labor-intensive audits can be performed without laying a hand on the network facilities to be audited, and the CSRIC best practice upon which our standard is based does not specify the form of audit recommended. Covered 911 Service Providers might not have integrated operations systems to perform this task, but they do have cable records and circuit inventory databases that can be used. CenturyLink, for instance, notes that while it "does not formally 'lock down' 911 circuits in order to preserve the ability to readily perform maintenance or emergency work on them," it does have a process in place to "verify that any design changes will not adversely affect 911 network diversity or other functionality."[215] In light of the above, we decline to adopt detailed standards – beyond those discussed above – governing how Covered 911 Service Providers must conduct these audits.

93. *Frequency of Audits.* The *911 Reliability NPRM* sought comment on how often 911 reliability certifications should be submitted.[216] For the reasons discussed below, we conclude that a requirement that Covered 911 Service Providers conduct annual audits of their 911 circuits coupled with a requirement for submission of annual certifications best serves the public interest. We agree with those commenters who note that regular auditing of critical 911 circuits can significantly improve network reliability[217] and we conclude that annual auditing of 911 circuits and network monitoring links is

[206] *See* AT&T Comments at 12-13.

[207] *See id.* at 11-12.

[208] *See* AT&T Ex Parte Notice at 1 (June 3, 2013).

[209] AT&T Ex Parte Notice at 1 (June 27, 2013).

[210] Verizon Comments at 6.

[211] Verizon Ex Parte Notice at 1 (July 3, 2013).

[212] *Id.*

[213] Frontier Comments at 8-9; CenturyLink Reply Comments at 7.

[214] *See* CenturyLink Reply Comments at 7.

[215] *See* CenturyLink Ex Parte Notice at 3-4 (June 20, 2013).

[216] *911 Reliability NPRM*, 28 FCC Rcd at 3432 ¶ 40.

[217] *See* NENA Comments at 10 ("With respect to both [selective router]-to-PSAP trunks and redundant ALI datalinks, NENA believes that regular auditing of physical path diversity can significantly improve 9-1-1 system reliability."); APCO Comments at 3 (urging the Commission to require "specified levels of physical diversity for 9-1-1 circuits," consistent with CSRIC best practices).

necessary to prevent a loss of diversity in these critical circuits due to routine circuit rearrangements between audits.

94. The relevant CSRIC best practice advises network operators to "periodically audit the physical and logical diversity called for by network design and take appropriate measures as needed," but it does not recommend a specific interval for 911 circuit audits.[218] Some commenters, primarily Covered 911 Service Providers, contend that annual circuit audits are unnecessary and that reliable 911 service may be adequately maintained through audits every three years,[219] or on some other schedule.[220] Public safety commenters, however, recommend more frequent audits, combined with an obligation to quickly address any vulnerabilities that those audits reveal. New York City and the Pennsylvania Public Utility Commission both favor annual audits.[221] Fairfax County proposes audits at least every two years but notes that this recommendation is contingent on "the relative stability of the circuit routes after any remediation" and assumes that "service provider process controls are in place to establish 'lock downs' on the circuit routes."[222] The derecho experience, however, revealed that multiple service providers not only failed to detect serious vulnerabilities in their 911 networks, but could not even identify critical circuit routes until long after the outages occurred.[223] We conclude from this experience, and from comments indicating that service providers' current circuit-auditing practices are often insufficient to provide assurances of reliable service,[224] that a more rigorous approach is warranted.

95. Moreover, our experience reviewing thousands of NORS outage reports since 2004 shows that communications circuits, including 911 circuits, are subject to periodic, unpredictable reconfiguration to satisfy a variety of business and operational needs.[225] These reconfigurations can cause a previously diverse 911 circuit to be configured without diversity, which imposes a serious risk to 911

[218] *See* CSRIC Best Practice 8-7-0532, *available at* https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=8-7-0532 (emphasis added).

[219] *See* Frontier Comments at 9 (arguing for circuit audits every three years on grounds that annual audits would not be necessary if service providers tag critical circuits to prevent inadvertent rearrangement); *cf.* Verizon Ex Parte Notice at 1 (July 3, 2013) (stating that Verizon plans to perform diversity reviews every three years).

[220] *See* Century Link Ex Parte Notice at 1 (Sept. 18, 2013) (stating that it would take "approximately 24 months to audit all the 911 circuits in its network"); AT&T Reply Comments at 8 (supporting a requirement that 911 service providers "certify annually that they conduct computerized audits consistent with industry best practices," but not specifying an interval for each audit of its network).

[221] *See* Pennsylvania PUC Comments at 13 (supporting "annual auditing for physical diversity to avoid single points for routine 911 circuits," with remediation complete by the end of the second year); City of New York Reply Comments at 2 (supporting "[a]nnual auditing of 911 trunked circuits and other designated high priority circuits to ensure physical diversity" in dense urban and suburban areas).

[222] Fairfax County Comments at 4. *See also* City of Falls Church Comments at 1 (joining in Fairfax County Comments); City of Alexandria Comments at 5 (supporting "periodic, mandatory circuit auditing" by 911 service providers).

[223] *See* Derecho Report at 21 (stating that "it is clear to the Bureau that Verizon was not fully aware of the routing of its own critical circuits until a considerable time after they failed").

[224] *See* Mission Critical Partners Comments at 6 ("Our experience in various locations in the country has been that many carriers are reluctant or unwilling to provide detailed physical circuit maps due to the failings that they reveal.")

[225] *See* FCC's Public Safety and Homeland Security Bureau Reminds Telecommunications Service Providers of Importance of Implementing Advisory Committee 911 and Enhanced 911 Services Best Practices, *Public Notice*, DA 10-494, 25 FCC Rcd 2805 (PSHSB rel. March 24, 2010) (Observing that "[t]hrough an examination of network outage reports filed through [NORS], the Bureau has observed a significant number of 911/E911 service outages caused by a lack of diversity that could have been avoided at little expense to the service provider").

reliability. We conclude that annual circuit diversity audits will reveal conditions like these, and enable providers to take steps to address any such issues in a timely manner.

96. Further, we find that any costs associated with annual audits are incremental and modest, at best, as many service providers claim that they already have implemented similar processes. For example, while Verizon proposes circuit audits every three years, it notes that it had "almost completed" auditing its entire 911 network *less than* a year after the derecho.[226] Other service providers comment that more frequent audits would require additional staff time.[227] Even if true, the derecho and associated outages show that these additional resources may well be necessary to fulfill Covered 911 Service Providers' responsibility to provide dependable service when it matters most. While there may be startup costs associated with these needed improvements, service providers that have already implemented automated circuit audits demonstrate that the incremental cost of each audit decreases once the system has been developed.[228] Even if other service providers, particularly smaller entities with fewer resources, do not currently have such systems in place, the two-year phase-in of our certification allows time to implement more efficient auditing mechanisms that will reduce costs over time while increasing network reliability. Once internalized, these efficiencies will address service provider concerns that one audit may not be completed by the time the next certification is due.[229] Moreover, the tagging of circuits to prevent inadvertent rearrangement over time in accordance with our rules will further serve to minimize the time required for future audits.[230] Accordingly, we are persuaded that annual 911 circuit audits are necessary to ensure that necessary diversity of 911 circuits and, in turn, promote the reliability of our 911 communications system.

97. *Corrective Measures.* Under the rules we adopt today, Covered 911 Service Providers must certify annually whether they have, within the past year, audited the physical diversity of critical 911 circuits or equivalent data paths to each PSAP they serve, tagged those circuits, and eliminated single points of failure in these circuits. In lieu of eliminating single points of failure, providers also may certify that they have taken specific, alternative measures reasonably sufficient to mitigate the risk of insufficient physical diversity. While physical diversity always results in higher reliability, we are persuaded by AT&T and others that the costs of achieving physical diversity inflexibly in every instance would be overly burdensome.[231] We are also sympathetic to NTCA's arguments that the relevant 911 infrastructure is frequently owned and operated by a separate service provider. Hence, we decline to adopt uniform performance requirements specifying physical diversity for all critical 911 circuits, but we require

[226] *See* Verizon Comments at 6 (noting in May 2013 that within the past year "Verizon conducted network design reviews of PSAP trunking and ALI links for diversity for all Maryland and Virginia PSAPs" and "has almost completed similar reviews of PSAP trunking throughout its footprint").

[227] *See* Frontier Comments at 9 (arguing that annual circuit audits would require the work of nine full-time employees); CenturyLink Ex Parte Notice at 1 (Sept. 18, 2013) (arguing that it would take seven employees twenty-four months to audit and tag all of its critical 911 circuits).

[228] *See* AT&T Ex Parte Notice at 1 (June 27, 2013) (noting that that "after the initial development of the tool is complete, there are minimal incremental costs to operating and maintaining" its automated Diversity Analysis Reporting Tool (DART)); Verizon Ex Parte Notice at 1 (July 3, 2013) (acknowledging that the automated process it is developing "may require slightly less time" than previous manual audits).

[229] *See* Century Link Ex Parte Notice at 1 (Sept. 18, 2013).

[230] *See* Fairfax County Comments at 4 (noting that 911 circuits may be relatively stable between audits if service providers "lock down" diverse circuits); Frontier Comments at 9 ("Once all critical circuits are flagged and identified within the database, regional engineers that are planning changes within the network would review the system records and identify critical circuits that reside on facilities and/or equipment they are proposing to change.").

[231] *See* AT&T Comments at 19-20; Frontier Comments at 10-11; Alaska Communications Systems Comments at 3; Verizon Comments at 12.

Covered 911 Service Providers to explain why measures short of physical diversity are reasonably sufficient to ensure reliable 911 service in individual cases.

98. Service providers have a number of flexible methods at their disposal to satisfy the certification requirement and mitigate the risks of circuit failure, even where ensuring complete physical diversity may not be feasible. Because the decision whether to order diverse access through multiple selective routers, or the functional equivalent, typically rests with the PSAP and is driven by budgetary and other local concerns,[232] we agree that service providers should not be inflexibly required to install costly, redundant circuits where a PSAP has not ordered that level of service. They will be required, however, to audit their critical 911 circuits for physical diversity as our rules set forth. Verizon, for example, states that less than 20 percent of the PSAPs it serves have only a single selective router,[233] although the proportion may be higher in rural areas where communities are spread farther apart.[234] As NENA notes, however, there are technologies and services that can help overcome the obstacles presented by the lack of physically diverse wireline facilities.[235] Thus, even where there is limited access to physical routes for critical 911 circuits,[236] service providers have many alternatives that can yield physically diverse service and the reliability it offers.

99. Moreover, while physical diversity may be impossible to achieve in a particular situation, logical diversity can often be achieved relatively easily and at modest cost, and could be reasonably sufficient in such circumstances to mitigate the risks associated with insufficient physical diversity. For example, a circuit audit might reveal that all 911 circuits to a PSAP terminate on a single circuit pack in a digital cross-connect system. It would not be costly or difficult to move some of these circuits to a different circuit pack, adding some measure of physical diversity without requiring a second selective router. As NENA points out, "in many cases the trunks connecting the selective router to its PSAPs' serving end offices do have *some* diversity, by virtue of dividing the trunk groups in two and sending each half along a different physical path."[237] Where a separate physical path is unavailable, 911 trunks can be spread out across diverse equipment in the central offices through which the trunks pass, providing a modest level of diversity. Similar methods can be applied to ALI links to make them more resilient. These measures may be considered reasonably sufficient to mitigate the risk of insufficient physical diversity, depending on the facts of individual cases.

100. *Cost Effectiveness.* Regarding costs of 911 circuit auditing, we note as an initial matter that our approach is likely to be cost-effective because it is has been designated a best practice by industry, via CSRIC.[238] Moreover, many Covered 911 Service Providers argue that such reviews are

[232] *See* Alaska Communications Systems Comments at 4-5 ("The decisions and funding commitments necessary to achieve [improved] redundancy and service resiliency are wholly within the province of the PSAP and its associated local governmental budgeting process."); NENA Reply Comments at 2 ("From the [selective router] to the served PSAP. . . NENA agrees with Alaska Communications Systems that route diversity should be the responsibility of 911 authorities or PSAPs."), Mission Critical Partners at 5.

[233] Verizon Comments at 11.

[234] *See* Alaska Communications Systems Comments at 3 ("In the Alaska bush, where there may not be a PSAP covering 150 or more communities, physical route diversity may not be possible, because there may be only a single facility or route serving a given bush location.").

[235] *See* NENA Reply Comments at 3 ("Today, a number of less-costly technologies such as microwave, free-space optical, encapsulated IP transport, and even lower-cost satellite service are available, and can meet PSAPs' needs for last mile redundancy."); EchoStar Comments at 3 ("Time and time again, satellite technology has demonstrated its ability to offer true path diversity to enable the continued availability of communications services.").

[236] See NTCA Comments at 6.

[237] *See* NENA Comments at 10 (emphasis in original).

[238] *See* ¶ 4, *supra*.

already part of their normal course of business.[239] Hence, the incremental costs to comply with the certification requirements we adopt today should be modest. However, we also believe that the costs should be narrowly tailored to the need to ensure reliability of the critical circuits at issue here. We turn now to a more detailed analysis of commenters' views on costs and their justification.

101. In our *NPRM* we estimated that the incremental cost to perform the additional audits annually for all of the PSAPs where they are not being performed at regular intervals would be roughly $2.2 million.[240] We further estimated that half of PSAPs served by dual selective routers are not currently subject to regular audits.[241] In light of comments indicating that Covered 911 Service Providers already perform regular diversity audits for many, but not all, critical 911 circuits,[242] we believe that the *NPRM*'s estimate is reasonable, and may, in fact, be conservative. However, based on the reliability concerns described above, we conclude that audits must be performed on *all* PSAPs, not just those that are served by dual selective routers.[243] In the worst case, where the single-stranded PSAP audits cost as much as those for PSAPs served by dual selective routers, we would expect the annual incremental cost of those audits to be about $4.5 million when based on the assumptions in the *NPRM*.[244]

102. A number of service providers estimated higher costs on the grounds that circuit audits take longer than the sixteen hours estimated in the *NPRM*.[245] Even assuming that these more conservative figures are accurate, however, we conclude that most of these costs are already being incurred by Covered 911 Service Providers and will decrease over time as their auditing practices improve. As commenters attest through their descriptions of existing practices,[246] it is more likely that only a segment of critical 911 circuits are not already subject to regular audits consistent with today's *Report and Order*, and the incremental cost to audit the remaining circuits on an annual basis is the more reasonable figure to use in an assessment of the burden imposed by our auditing requirement. Frontier, for example, estimates that "diversity reviews" of all its critical circuits would take approximately twenty-three hours per PSAP served.[247] Even if Frontier is correct, and if we continue to estimate that half of all critical 911 circuits are not currently audited each year, the incremental cost of our circuit auditing requirement across the

[239] *See* AT&T Comments at 11 ("Consistent with industry best practices, 9-1-1 circuit auditing is already a part of AT&T's standard operating procedure."); Frontier Comments at 8 ("Frontier has a team performing diversity reviews on network elements within central offices and outside plant fibers."); Verizon Comments at 6 ("[L]ast year, Verizon conducted network design reviews of PSAP trunking and ALI links for diversity for all Maryland and Virginia PSAPs. . . [and] has almost completed similar reviews of PSAP trunking throughout its footprint."); ATIS Comments at 10 ("[C]ommunication providers do recognize the importance of maintaining 9-1-1 circuit availability and have appropriate processes in place to meet established commitments to PSAPs.").

[240] *See 911 Reliability NPRM*, 28 FCC Rcd at 3432-33 ¶ 41. The *NPRM* based this calculation on the assumptions that critical 911 circuits serving approximately 1,750 PSAPs (half of those served by dual selective routers) would be audited annually at a cost of $1,280 per audit, for a total cost of $2,240,000.

[241] *See id.*

[242] *See* AT&T Comments at 11; Frontier Comments at 8; Verizon Comments at 6; ATIS Comments at 10.

[243] The *NPRM* assumed that each audit would take 16 hours at $80/hour and would only be conducted yearly on those PSAPs served by a 911 dual selective router configuration, which we estimated accounts for 50 percent of all PSAPs. *See 911 Reliability NPRM*, 28 FCC Rcd at 3432-33 ¶ 41.

[244] 3,500 audits (half of 7,000 PSAPs nationwide) * 16 hours each audit * $80 per hour = $4,480,000.

[245] *See* Verizon Comments at 11, Frontier Comments at 8-9.

[246] *See* AT&T Comments at 11, Frontier Comments at 8, Verizon Comments at 6, ATIS Comments at 10.

[247] *See* Frontier Comments at 8-10 (estimating a total of 18,660 hours to audit all critical circuits to "over 800 PSAPs nationwide," or 23.3 hours each). While Frontier's comments provide time estimates for auditing various components of the network (*e.g.*, end offices, ALI links and PSAP trunks), we use the aggregated number as a measure of the total incremental coast of our auditing requirement for comparison with estimates provided by other commenters.

nationwide network would be about $6.4 million.[248] Notably, Frontier comments that "once the information is audited it is included in a database and future audits should take less time on a going-forward basis."[249] Similarly, CenturyLink asserts that it would take seven employees twenty-four months to audit and tag all of its critical 911 circuits, at a cost of $1.3 million annually,[250] indicating that its current manual audits each require about twenty-nine hours of labor.[251] Yet CenturyLink also comments that it already "has processes in place to prevent adverse impacts to 9-1-1 network design . . . [and] verify that any design changes will not adversely affect 9-1-1 network diversity or other functionality,"[252] suggesting that it already bears at least some of the costs of auditing and tagging critical 911 circuits. Even if CenturyLink is correct that its *total* auditing costs would be $1.3 million annually, and even if all Covered 911 Service Providers incur the same expense – which is unlikely because some already perform automated audits and others are developing such processes – the annual *incremental* cost for all providers would be $8.1 million.[253] Verizon argues that each diversity audit requires 40 hours of engineering time,[254] in which case the total incremental cost would not exceed $11.2 million.[255] Verizon also states, however, that it already routinely audits all critical 911 circuits, even for PSAPs served by only a single selective router, and that it already is developing a more efficient auditing process.[256]

103. In any event, these estimates provide a range of $6.4 million to $11.2 million in annual incremental costs, even if we accept the industry view that critical 911 circuit audits require more time than we estimated in the *NPRM*. In light of comments from AT&T describing the "minimal incremental cost" of computerized audits[257] and from Frontier and CenturyLink indicating that even their existing auditing methods require less than 40 hours per PSAP,[258] however, we do not believe Verizon's estimate accurately represents the cost of our rules to the industry as a whole.[259] Furthermore, the two-year phase-in of our certification will allow all Covered 911 Service Providers to reexamine their existing circuit

[248] 3,500 audits * 23 hours each audit * $80 per hour = $6,440,000.

[249] Frontier Ex Parte Notice at 1 (July 3, 2013).

[250] CenturyLink Ex Parte Notice at 1 (Sept. 18, 2013).

[251] CenturyLink states that it serves 1,117 PSAPs and would require two years to audit those circuits. *See* CenturyLink Ex Parte Notice at 3 (June 20, 2013). If we accept these numbers, it follows that half, or 558 of those PSAPs, would be audited each year at a cost of $1.3 million or $2,330 per PSAP. This amounts to about 29 hours per PSAP if labor costs $80 per hour.

[252] CenturyLink Ex Parte Notice at 3 (June 20, 2013).

[253] 3,500 audits * 29 hours * $80 per hour = $8,120,000.

[254] *See* Verizon Comments at 11.

[255] 3,500 audits * 40 hours each audit * $80 per hour = $11,200,000.

[256] Verizon Comments at 11; Verizon Ex Parte Notice at 1 (July 3, 2013) (acknowledging that the automated process it is developing "may require slightly less time" than previous manual audits).

[257] AT&T Ex Parte Notice at 1 (June 27, 2013).

[258] *See* Frontier Comments at 8-9 (estimating about 23 hours per PSAP audited); CenturyLink Ex Parte Notice at 3 (June 20, 2013); CenturyLink Ex Parte Notice at 1 (Sept. 18, 2013) (estimating about 29 hours).

[259] Even if Verizon's higher cost estimate were correct, it would not change our conclusion that annual circuit audits are warranted in light of the public safety benefits of reliable 911 service. The expected benefit from only 10 percent of 911 calls (*i.e.*, those calls involving cardiac emergencies) by itself covers 66 percent of the incremental cost of a certification including annual circuit audits, even if we use Verizon's figures ($9.1 million value of one statistical life / $13.8 million cost of all certification elements including annual audits = 0.659). We therefore expect the total benefit from our rules to far exceed total incremental costs, even if Verizon's cost estimate were accurate. *See* ¶ 75, *supra*.

auditing practices and implement more efficient systems.[260] Accordingly, we conclude that the lower end of the industry range – about $6.4 million – is a reasonable estimate of the annual incremental cost of our circuit auditing requirement once the audits we require are put into practice.[261] Notably, these estimates reflects the cost of a "highly important" best practice that virtually all Covered 911 Service Providers claim to follow already to some degree.[262] The incremental cost of conducting circuit audits in conformance with our certification will be substantially less than the total cost, regardless of how it is calculated.

104. We recognize that these estimates are based on assumptions, and that some of these assumptions may not be true for all service providers. For example, small and rural carriers additionally argue that circuit-auditing obligations would have a disproportionate impact on providers without the necessary staff and resources.[263] Although we acknowledge that there will be costs associated with any circuit auditing requirement, we believe the approach we adopt minimizes those costs while providing Covered 911 Service Providers with the flexibility to manage their compliance burden in areas where they find it infeasible to implement remedies that bring them into full compliance with our critical 911 circuit diversity requirements. Thus, we conclude that the approach we adopt is cost-effective.

105. One commenter argues that if the Commission adopts regulatory mandates in this proceeding, it should "also identify federal funding sources to address the cost of compliance" and also "consider whether federal legislation would be necessary to assist 911 Service Providers in meeting the 911 reliability objectives."[264] Similarly, Frontier comments that "[i]f the Commission truly wants to provide diversity to every critical circuit it will need to make significant resources available to carriers to do so."[265] The *911 Reliability NPRM* inquired whether there should be a "mechanism for cost recovery beyond the 911 related tariff mechanisms already in place" for common carriers under Title II of the Communications Act.[266] Although some commenters assert that regulatory obligations with respect to circuit auditing and diversity would be prohibitively expensive without additional funding,[267] our analysis above shows that service providers already budget for many of the costs of the approach we adopt today and are unlikely to incur significant incremental costs to comply with certification requirements.[268] We

[260] *See* AT&T Ex Parte Notice at 1 (June 27, 2013). (describing the "minimal incremental costs" to performing circuit audits after development of its automated system); Verizon Ex Parte Notice at 1 (July 3, 2013) (acknowledging that the automated process it is developing "may require slightly less time" than previous manual audits); Frontier Ex Parte Notice at 1 (July 3, 2013) (noting that "future audits should take less time on a going-forward basis").

[261] We expect the costs to remediate diversity vulnerabilities to be a small percentage of the costs to perform 911 circuit audits. First, the costs to remediate diversity problems will, in most cases, involve reassigning circuits. These costs should be fairly small since the circuit audits will have already identified the places where additional diversity should be provided and circuit reassignments are routinely done with automated systems. Second, even though all 911 circuits will be audited, it is likely that only a fraction of those circuits will require remediation in light of service providers' claims that they already have processes in place to maintain 911 circuit diversity.

[262] *See* AT&T Comments at 11, Frontier Comments at 8, Verizon Comments at 6, ATIS Comments at 10; CenturyLink Ex Parte Notice at 3 (June 20, 2013).

[263] *See* Alaska Communications Systems Comments at 9 ("The regulatory burden of preparing and filing yet another Commission report is costly.").

[264] AT&T Comments at 11 n.8.

[265] Frontier Comments at 10-11.

[266] *911 Reliability NPRM*, 28 FCC Rcd at 3425 ¶ 23.

[267] *See* AT&T Comments at 11 n.8; Frontier Comments at 10-11.

[268] Furthermore, the standards that we have selected as the basis for the circuit diversity audits and associated certifications are based on those recommended to us by CSRIC and found by that body to be "highly important." Such "highly important" practices serve the vital purpose of improving the likelihood of emergency call completion, (continued….)

therefore disagree that these requirements amount to an extraordinary increase in costs, particularly in light of the option for service providers to employ reasonable alternative measures where physical diversity is not feasible. Accordingly, we decline at this time to consider additional sources of funding for compliance with the rules we adopt today.

2. Central-Office Backup Power

106. The *911 Reliability NPRM* noted that "reliable central office backup power is essential for communications during large-scale emergencies, and backup power failures in [central offices] can disable 911 communications services for an entire community."[269] It posed a range of questions regarding backup power, including whether all central offices should be required to have dedicated backup power, what constitutes "adequate" backup power, and what level of testing and maintenance is necessary to ensure reliability.[270] The *NPRM* also acknowledged "what constitutes a 'central office' can vary to some extent by service provider and location," and that some facilities may require a greater degree of backup power than others.[271] Multiple CSRIC best practices address backup power issues such as generator design and configuration,[272] and appropriate testing and maintenance.[273] These best practices also provide that all critical infrastructure facilities should be supported by backup power systems such as batteries, generators, and fuel cells.[274]

107. The rules we adopt today require Covered 911 Service Providers to certify annually whether they have sufficient, reliable backup power in any central office that directly serves a PSAP to maintain full service functionality, including network monitoring capabilities, for at least 24 hours at full office load. Further, we require the especially critical central offices that host selective routers to be equipped with at least 72 hours of backup power at full office load. The specified level of backup power may be provided through fixed generators, portable generators, batteries, fuel cells, or a combination of those or other such sources so long as it meets the applicable certification standard.

108. If that level of backup power is not feasible at a particular central office that directly serves a PSAP or hosts a selective router, the certification will be required to indicate this. The service provider must briefly state why it is not feasible and describe the specific alternative measures it has taken to mitigate the risk associated with backup power configurations that fail to satisfy the certification standard. Covered 911 Service Providers may also certify that they believe this element of the certification is not applicable to their network, although they must explain why it is not applicable. As noted above with regard to covered entities, a central office "directly serves a PSAP" if it (1) hosts a selective router or ALI/ANI database (2) provides equivalent NG911 capabilities, or (3) is the last

(Continued from previous page)
with caller information, to the appropriate response agency, ensuring access to emergency communications for all callers. *See* CSRIC II Working Group 6, Best Practice Implementation Final Report at 7-8 (January 2011), *available at* http://transition.fcc.gov/pshs/docs/csric/WG6-Best-Practice-Implementation-Final-Report.pdf.

[269] *911 Reliability NPRM*, 28 FCC Rcd at 3421 ¶ 14.

[270] *See id.* at 3434-37 ¶¶ 44-46.

[271] *Id.* at 3435 ¶ 46.

[272] *See* CSRIC Best Practice 8-7-5281 (disapproving of interdependent generators); CSRIC Best Practice 8-7-0657, *available at* https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=8-7-0657 ("Network Operators, Service Providers and Property Managers should design standby generator systems for fully automatic operation and for ease of manual operation, when required.").

[273] *See* CSRIC Best Practice 8-7-0662, *available at* https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=8-7-0662 ("Network Operators, Service Providers and Property Managers should exercise power generators on a routine schedule in accordance with manufacturer's specifications. For example, a monthly 1 hour engine run on load, and a 5 hour annual run.").

[274] CSRIC Best Practice 8-7-5058, *available at* https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=8-7-5058.

service-provider facility through which a 911 trunk or administrative line passes before connecting to a PSAP. Service providers must also certify (1) that they test and maintain all backup power equipment in all central offices directly serving PSAPs in accordance with the manufacturer's specifications, per CSRIC best practice,[275] (2) that they adhere to CSRIC best practices[276] regarding fully automatic, non-interdependent generators that can be started manually if necessary,[277] and (3) that they retain records of backup power deployment and maintenance for confidential review by the Commission, upon request, for two years. If the specified standards related to testing and tandem generator configurations cannot be met, the service provider must briefly state why it is not feasible to meet them and describe the specific alternative measures it has taken to mitigate the risk associated with the failure to satisfy the certification standards.

109. Because different central offices present different backup power challenges and a single solution may not be suitable for all,[278] we allow Covered 911 Service Providers to certify and describe reasonable alternative measures on a case-by-case basis. For these reasons, rather than codifying existing best practices as prescriptive rules, the certification requirement we adopt today allows 911 service providers flexibility to maintain adequate central-office backup power based on best practices and reasonable alternatives to suit site-specific circumstances.

110. Several communications providers, even RLECs that presumably have more limited resources, note that they already maintain sufficient reserves of backup power to compensate for commercial power outages in harsh climates and geographies.[279] Frontier, for example, "has reviewed and updated its generator plan as part of its overall performance maintenance plan and also has policies for generator usage in emergency situations."[280] Frontier currently "sets an internal standard of having

[275] *See* CSRIC Best Practice 8-7-0662, *available at* https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=8-7-0662 ("Network Operators, Service Providers and Property Managers should exercise power generators on a routine schedule in accordance with manufacturer's specifications. For example, a monthly 1 hour engine run on load, and a 5 hour annual run.").

[276] *See* CSRIC Best Practice 8-7-0657, *available at* https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=8-7-0657 ("Service Providers . . . should design standby generator systems for fully automatic operation and for ease of manual operation, when required."); CSRIC Best Practice 8-7-5281, *available at* https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=8-7-5281 ("Service Providers . . . with buildings serviced by more than one emergency generator should design, install and maintain each generator as a standalone unit that is not dependent on the operation of another generator for proper functioning, including fuel supply path.").

[277] *See* NATOA Comments at 6.

[278] *See* Western Telecommunications Alliance Comments at 10; Frontier Comments at 13; CenturyLink Reply Comments at 9-11.

[279] *See* Alaska Communications Systems Comments at 10-11 ("Reliable commercial power is unavailable in many areas of Alaska that ACS serves, and ACS therefore maintains significant backup power capabilities, both in Anchorage and throughout the state. ACS maintains generators at critical locations throughout the state, as well as its own, on-site fueling station that it can use to supply and resupply the necessary fuel to keep these generators operating. In addition, many ACS central offices have battery backup facilities that offer an additional source of emergency power, should it be needed."); NTCA Comments at 7 ("RLECs typically have on-hand uninterruptible power supply systems, backup batteries, and portable and on-site generators.").

[280] *See* Frontier Comments at 3, 11. ("For Base Unit Central Offices Frontier is in compliance with CSRIC best practice 8-7-5281 and has a single stationary generator with a single fuel source. Frontier has a performance maintenance plan that it follows for backup power, whereby it follows the backup power test procedures and records the results. The plan incorporates very specific and detailed AC generator, battery and DC power system standards, including testing the backup generators under an actual office load. Stationary generators are to be tested monthly with an annual "blackout" test also incorporated.").

three to four hours of backup power available at a site with a stationary generator and up to eight hours available for a site that requires a portable generator," although "[t]hese standards may vary depending upon individual state requirements."[281] Verizon comments that "almost all" of its central offices "are engineered to have on-site, fixed generators with 72-hour fuel reserves as well as battery reserves. When a generator is present, the battery reserve is generally designed for at least three hours, and sometimes more, depending on state and local standards or needs. Otherwise, the battery reserve is designed for over eight hours to allow time for a Verizon technician to arrive on site and connect a portable generator."[282] Verizon also "maintains a thorough testing and maintenance practice for its backup power," including both monthly and annual generator tests and annual battery discharge tests.[283] AT&T declares that it has "fixed generators in 88 percent of its central offices, backup batteries at all central offices, and a fleet of portable generators that can be mobilized on a moment's notice."[284] AT&T also describes a rigorous backup power testing program based on manufacturer-recommended schedules, just as we choose today as the certification standard for backup power testing.[285] According to CenturyLink "there are numerous best practices associated with backup power that CenturyLink generally follows to ensure functionality in an emergency, including engine maintenance, battery maintenance, battery backup requirements, fuel reserves, just to name a few."[286] We conclude from these comments that most Covered 911 Service Providers are currently implementing in the normal course of business the practices that we call for as part of the backup power certification process we adopt today. But while these filings imply general conformance to backup power standards, the failures observed in the derecho cause us to conclude that additional Commission oversight is needed, particularly as it relates to vital emergency services.

111. Public-safety commenters strongly support minimum backup-power requirements, or at least an obligation to certify that backup power is adequate and properly maintained.[287] NENA, for example, states that "a prudent standard would begin at a minimum of 24 hours of uninterruptable backup power" and that especially critical facilities should have as many as 120 hours available.[288] According to Fairfax County, "mandating backup power equipment testing and maintenance, along with supporting

[281] Frontier Comments at 11. State requirements for central-office backup power vary based on the number of lines an office serves, whether it has a permanently installed generator, and other factors. Alabama, for example, provides that "[c]entral offices that have 24-hour maintenance coverage or have an automatic start engine alternator shall provide a minimum of three hours of battery reserve [and] [a]ll other central offices shall have a minimum of eight hours of battery reserve." Colorado requires "a minimum of four hours of backup power or battery reserve rated for peak traffic load" and a "mobile power source . . . that can be delivered and connected within four hours," as well as a permanent auxiliary power unit in all toll or tandem switching offices and central offices with the capacity for more than 10,000 access lines. In Iowa, "[e]ach central office shall contain a minimum of two hours of battery reserve" but for offices without permanent generators, "there shall be access to a mobile power unit with enough capacity to carry the load which can be delivered on reasonably short notice and which can be readily connected," and "[a]n auxiliary power unit shall be permanently installed in all toll centers and at all exchanges exceeding 4,000 access lines." *See* CenturyLink Ex Parte Notice, Exhibit A (June 20, 2013).

[282] Verizon Comments at 3.

[283] *See id.* at 3-4.

[284] *See* AT&T Comments at 16.

[285] *See id.* at 17.

[286] CenturyLink Reply at 8.

[287] *See* California PUC Comments at 9 (stating that "CPUC recommends that the FCC adopt specific minimum back-up power requirements or standards for central offices and other network locations necessary to ensure the provisioning of 911 service."); City of Alexandria Comments at 6 ("Assuring adequate backup power for every telephone central office facilities supporting regional 911 services should be part of every service level of agreement between the PSAP and the emergency communication service providers.").

[288] NENA Comments at 12.

documentation of same, is the most logical way to improve 911 reliability and provide an ongoing level of assurance that the appropriate best practices are being implemented and carried through on a routine basis."[289] While the Edison Electric Institute "believes that adoption by the Commission of proscriptive rules or standards is not an ideal solution to address reliability deficiencies and backup power issues," it does support a certification approach, arguing that it "will serve the dual function of establishing a transparent means for ensuring service providers routinely meet a certain threshold for backup power, and providing electric utilities and other CII users of communications networks up-front knowledge as to the reliability of a given network."[290]

112. Service providers, by contrast, argue that they should retain flexibility to determine the best backup power strategy for each service and facility, and that the Commission underestimates the cost of complying with backup power mandates.[291] AT&T, for instance, argues that "a mandate to provide on-site backup power in every central office would eliminate . . . necessary flexibility and undermine provider efforts to provide backup power in the most efficient possible manner." Commenters with diverse points of view recommended that our backup power rules provide flexibility to address the peculiarities of individual central office backup power situations.[292] Commenters also note that "standards may vary depending upon individual state requirements" and that backup power problems and requirements are not uniform nationwide.[293] Western Telecommunications Alliance adds that "location and likely weather conditions affecting an area"[294] will affect the feasibility of a achieving a particular backup power standard at a site.

113. The certification approach for backup power that we set forth today provides Covered 911 Service Providers with the flexibility to use alternative measures where the specified level of backup power is not feasible under the circumstances, so long as they describe those alternative measures and demonstrate that they are reasonably sufficient to mitigate the risk of failure. This process allows Covered 911 Service Providers the flexibility they seek to, among other things, "account for state and local geography, population density, and zoning and environmental laws,"[295] while reserving authority to order remedial action where alternative measures are not reasonably sufficient to ensure reliable 911 service. For example, fuel storage, zoning and noise ordinances may limit the placement of generators, thereby justifying a conclusion that strict adherence to the backup power standards set forth in our certification requirement is not feasible.[296]

---

[289] *See* Fairfax County Comments at 6.

[290] *See* Edison Electric Institute Comments at 7-8.

[291] *See* Frontier Comments at 12 ("Frontier has already spent considerable expense to develop its backup power plan and additional mandates for backup power may also prove to be cost prohibitive without further support.").

[292] *See* Virginia State Corporation Commission Comments at 7 (The Virginia State Corporation Commission has suggested that a monolithic, prescriptive set of regulations will not "be sufficiently detailed to address all the necessary operational parameters and situations."); Pennsylvania PUC Comments at 15 ("The Pa. PUC strongly supports allowances for waivers for good cause shown, particularly given the FCC's recognition of the differences between central offices in a large metropolitan area compared to a smaller rural area."); California PUC Comments at 10; CenturyLink Reply Comments at 4-5.

[293] Frontier Comments at 11 n.20, 13 ("Fourteen of Frontier's 27 states of operation have some sort of regulation or requirement with respect to backup power.").

[294] *See* Western Telecommunications Alliance Comments at 9.

[295] *See* California PUC Comments at 10, 12

[296] *See* NTCA Comments at 7; Western Telecommunications Alliance Comments at 9 ("The appropriate size and capacity of such batteries and generators, as well as the suitable frequency of their testing, depends much upon the location and likely weather conditions affecting an area. For example, a mountain community likely to be snowed in for weeks during certain winters will need different backup power capacities and testing arrangements than a community on the Great Plains that is subject to a spring tornado every decade or so.").

114. Some commenters urge us to "look more broadly to all sites and critical nodes, and to be mindful of the need for adequate backup power at each network location."[297] However, because this proceeding focuses on the critical infrastructure serving PSAPs that the *Derecho Report* identified as a source of failure, rather than on call origination and other network nodes, we limit backup-power requirements to those central offices that could create choke points between Covered 911 Service Provider networks and PSAPs. Although the *NPRM* suggested that backup-power requirements might apply to all central offices,[298] we conclude that a targeted emphasis on central offices that directly serve PSAPs or host selective routers is most appropriately tailored to the problem identified in this proceeding. Because the failure of one selective router could disrupt service to an entire region and prevent re-routing of 911 calls to other PSAPs, we consider the central offices that host selective routers to be among the most important facilities in the nation's 911 infrastructure, and especially critical to public safety.[299] By focusing our certification requirements on the central offices associated with reliable 911 service and prioritizing the most critical of those facilities, we seek to limit burdens on service providers and promote investment in backup power where it is most needed for public safety.

115. A number of commenters expressed opinions about the standards that should underlie backup power certification. For facilities such as central offices that host a selective router, NENA asserts that "a minimum of 72 hours and a normal range of 120 hours of backup power would be considered prudent."[300] The Pennsylvania PUC recommends that we "require backup power in any [central office] sufficient for 72 hours."[301] Mission Critical Partners recommends that the "Commission require, by rulemaking, the 911 service entities self-certify that critical facilities are compliance with National Fire Protection Association (NFPA) 110 standards *at a minimum*."[302] Fairfax County recommends that we base our certification standard on a formula, to be developed in the future, that would calculate the likelihood that a particular central office's backup power implementation would fail to perform during a loss of commercial power.[303] While this approach has the advantage of being directly

[297] Edison Electric Institute Comments at 7. *See also* NATOA Comments at 6 (noting that "remote terminal access is also important during emergencies"); Pennsylvania PUC Comments at 18-24 (discussing battery backup for customer premises equipment (CPE) used to provide VoIP services).

[298] *911 Reliability NPRM*, 28 FCC Rcd at 3437 ¶ 52.

[299] Moreover, the number of central offices with selective routers is only a small fraction of the total nationwide. AT&T, the only service provider that supplied such information, comments that it operates 172 offices that contain selective routers, AT&T Comments at 16 (noting that AT&T "has 172 offices that contain 9-1-1 Tandem Selective Routers"), and provides 911 service to approximately 3,200 PSAPs. *Id.* at 2. If this proportion is consistent among all Covered 911 Service Providers – and the record contains no reason to believe it is not – we estimate that there are about 376 central offices that host selective routers nationwide. (172 selective routers/3,200 AT&T PSAPs = 0.05375 selective routers per PSAP. FCC records indicate that there are at most 7,000 PSAPs nationwide, in which case 376 selective routers would be required to serve all PSAPs (0.05375*7,000 = 376.25).) This suggests that each selective router serves, on average, nineteen PSAPs, (3,200 PSAPs/172 selective routers = 18.6 PSAPs per selective router), and underscores just how critical each central office with a selective router is to the nation's 911 network.

[300] *Id.*

[301] Pennsylvania PUC Comments at 14.

[302] *See* Mission Critical Partners Comments at 10 (emphasis in original). NFPA 110 standards, however, are primarily intended for application by manufacturers of communications equipment, not owners and operators of communications networks. *See* National Fire Protection Association, NFPA 110: Standard for Emergency and Standby Power Systems, *available at* http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=110&DocNum=110 ("This Standard covers installation, maintenance, operation, and testing requirements as they pertain to the performance of the emergency power supply system, including power sources, transfer equipment, controls, supervisory equipment, and all related electrical and mechanical auxiliary and accessory equipment.").

[303] *See* Fairfax County Comments at 6.

applicable to a particular site, it could lead to a burdensome and complicated compliance process for Covered 911 Service Providers.

116. We agree with commenters who note that central offices serve a variety of functions in the 911 network and should maintain the highest levels of backup power where a failure would be most likely to affect public safety. We therefore adopt a dual standard with 72-hour backup required at central offices hosting selective routers and 24-hour backup at all other central offices that directly serve PSAPs. These numbers are consistent with the recommendations of public safety commenters,[304] and many Covered 911 Service Providers indicate they are currently maintaining similar levels of backup power in the normal course of business.[305] As Pennsylvania PUC recommends, we allow flexibility to satisfy that standard using a variety of means;[306] thus, Covered 911 Service Providers may employ fixed generators, portable generators, batteries, or a combination of other such sources to meet the applicable level of backup power. However, to the extent that the provider is relying on portable sources, we will require that such sources be readily available within the time it takes the batteries to drain, notwithstanding potential loss of commercial power and demand for generators elsewhere in a Covered 911 Service Provider's network.

117. *Testing Standards.* The Pennsylvania PUC calls for full-load testing pursuant to the CSRIC best practice that is the basis for the standard.[307] NATOA recommends that generators should be tested under electrical load for approximately 20 minutes.[308] While these recommendations might be appropriate for certain sites, we find that they are too narrow for general application. The record reflects that industry's practice and public safety's preference in this area are reasonably well aligned. Hence, we require Covered 911 Service Providers, consistent with CSRIC best practice,[309] to certify that they test their backup power equipment according to the relevant manufacturers' specifications. This approach accounts for differences in equipment and facilities while ensuring that backup power assets are properly maintained. Pennsylvania PUC, similar to NATOA and City of New York,[310] calls for the site load approach to testing backup equipment in which the central office is switched off commercial power and left to run on backup power alone.[311] Although this method of testing may well be preferable in some situations, we decline to adopt this standard in our certification approach as other approaches can be used at lower risk.

118. NATOA and Pennsylvania PUC also recommend that tandem generators be electronically separated to ensure that failure of one generator does not cause the other to fail.[312] We

[304] *See* NENA Comments at 12; Pennsylvania PUC Comments at 14.

[305] *See* Verizon Comments at 3.

[306] *See* Pennsylvania PUC Comments at 14 ("The 911 Service Providers should be responsible for determining what sole or mixed reliance on uninterruptible power supply, batteries, and backup generators are the most effective means for powering any given central office, network facility or equipment so long as its meets a predetermined minimum time period.").

[307] *See* Pennsylvania PUC Comments at 16.

[308] *See* NATOA Comments at 5.

[309] *See* CSRIC Best Practice 8-7-0662, *available at* https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=8-7-0662 ("Network Operators, Service Providers and Property Managers should exercise power generators on a routine schedule in accordance with manufacturer's specifications. For example, a monthly 1 hour engine run on load, and a 5 hour annual run.").

[310] *See* City of New York Reply Comments at 2 (recommending "annual full load testing of central office backup power battery systems" and "quarterly full load testing of central office backup power generator systems").

[311] *See* Pennsylvania PUC Comments at 15

[312] *See* NATOA Comments at 5. Pennsylvania PUC Comments at 15.

agree and note that this is a CSRIC best practice[313] and that interdependent tandem generators were a primary cause of the failure of Verizon's central office backup power during the June 2012 derecho.[314] Accordingly, we will require the certification to confirm whether the 911 provider employs stand-alone backup power sources. As with circuit diversity, however, we will afford 911 providers an opportunity to demonstrate that alternative measures upon which they rely (*e.g.*, load shedding[315]) are reasonably sufficient to mitigate the risk of failure. Some commenters note that there are a variety of solutions available to shed electrical loads, and that some are more costly than others.[316] As with other aspects of the backup power certification, we do not specify a mandatory method of load shedding so long as a Covered 911 Service Provider demonstrates that its approach satisfies the foregoing standard of reliability.

119. *Cost Effectiveness.* In arriving at the cost estimates in our *NPRM*, we estimated costs for having fixed generators, or portable generators, available in all central offices; the costs for testing batteries; the costs for generator testing; the costs for repairing generators after failing tests; and the costs for rectifying tandem generator configurations where the failure of one generator results in the complete loss of backup power. In our *NPRM* we estimated that the incremental cost incurred to perform backup power certifications, including remediation, ranges from $11.7 million to $37.5 million depending on whether we require fixed generators at all central offices.[317] We include no such requirement in today's *Report and Order*, meaning that there would be no incremental costs for central offices appropriately provisioned with portable generators. As a result, we estimate the cost to conform to our backup power standards is much closer to $11.7 million than $37.5 million.[318]

120. The approach we adopt here will also significantly reduce the cost of compliance by covering only central offices directly serving PSAPs or hosting selective routers or ALI databases,[319] and allowing alternative measures where the specified level of backup power is not feasible. Limiting these requirements to central offices that directly serve PSAPs reduces our estimate of cost by 72 percent, from $11.7 million to about $3.3 million.[320]

121. Furthermore, industry comments suggest that Covered 911 Service Providers have already undertaken most of these measures. As commenters attest,[321] it is more likely that only a small fraction of central offices serving PSAPs do not adhere to the backup power standards we adopt today, and the incremental cost to adopt these standards at the remaining sites is the more reasonable figure to

[313] *See* CSRIC Best Practice 8-7-5281.

[314] *See Derecho Report* at 16-17; Fairfax County Comments at 6; Virginia State Corporation Commission Comments at 7.

[315] "Load shedding" refers to the process of diminishing the electrical load carried by an electrical power source, for example a battery or a generator.

[316] *See* CenturyLink Reply at 10-11 (discussing cost difference between manual and automated load-shedding systems and stating that a requirement for automated load shedding could be "significantly more costly" than estimated in the *NPRM*).

[317] *See 911 Reliability NPRM*, 28 FCC Rcd at 3438-39 ¶ 57.

[318] As noted below, we believe the actual cost will be significantly less than even the lower estimate in the *NPRM*. *See infra*, ¶ 130.

[319] We estimate that there are approximately 25,000 central offices in the United States and that approximately 7,000 of those central offices serve PSAPs; thus, limiting backup power requirements to only those offices directly serving PSAPs could focus service providers' efforts and costs on about 28 percent (7,000/25,000 = 0.28) of all central offices.

[320] 100% - 28% = 72%. $11.7 million * 72% = $3.276 million.

[321] *See* Alaska Communications Systems Comments at 10–11; NTCA Comments at 7; Frontier Comments at 11; Verizon Comments at 3-4; AT&T Comments at 16-17; CenturyLink Reply Comments at 8.

use in an assessment of the burden imposed by these rules. For example, virtually all 911 service providers that submitted comments claimed that they either have fixed generators deployed in a vast majority of central offices or have timely access to portable generators in the event of battery exhaustion during a commercial power outage.[322] Hence, the incremental cost to have portable generators available within a reasonable time in all central offices where our certification standard requires them to be available should be negligible. Even if we assume that 25 percent of all central offices that directly serve a PSAP lack a fixed generator and that 1 percent[323] of those central offices do not have access to a portable generator, we calculate the incremental cost of our rule to be about $525,000 if the cost of a portable generator is $30,000.[324]

122. *Generators (including Portable Generators) for Central Offices Serving PSAPs:* Verizon contends that the cost estimate for backup generators in the *NPRM* is "off by a factor of ten" and that "[a] generator that can produce sufficient power for an average Verizon [central office] costs around $1 million if purchased or around $50,000 per month if leased."[325] These estimates, however, represent the cost of a large, fixed generator. We note that, while our *NPRM* includes an estimate of fixed generator costs, the cost-benefit analysis in the *NPRM* also assumed that portable generators could be used, which lowers costs.[326] In that *NPRM*, we assumed that the cost of a portable generator was $30,000.[327] Verizon additionally states that an 800 kilowatt portable generator costs about $300,000.[328] But, according to Verizon, these are costs to provide generators for an "average Verizon CO" and, by Verizon's own admission, it has generators deployed in "almost all"[329] of its central offices already. If any central offices that serve PSAPs lack fixed generators, they are likely to be smaller facilities that serve fewer lines and require less power than an "average" central office. Thus, we disagree that cost estimates like Verizon's – which reflect the total cost of equipment that is already likely to be installed in key facilities – suggest that the incremental cost estimates in the *NPRM* were not reasonably accurate.

123. Similarly AT&T argues that the cost estimate in the *NPRM* "fails to account for the full panoply of costs involved in purchasing, installing, and maintaining permanent generators and fuel tanks," and "fail[s] to account for the engineering and labor costs to install these items (including possible retrofitting of COs to accommodate the equipment)."[330] While we agree that the costs estimated in the *NPRM* for a large, fixed generator are less than what some commenters have suggested, these costs are inapplicable because we are not requiring fixed generators. AT&T also attests that 88 percent of its central offices have both batteries and fixed generators deployed and that it has the "ability to effectively

[322] *See* Verizon Comments at 3-4; Frontier Comments at 11; AT&T Comments at 16.

[323] In the *NPRM*, we assumed that 5 percent of the central offices do not have access to a portable generator within the time it takes for the batteries to drain. *See 911 Reliability NPRM*, 28 FCC Rcd at 3437 ¶ 52. Based on comments indicating that virtually all 911 service providers have portable generators available where fixed generators are not installed, we believe that estimate is too high, and that 1 percent is more accurate.

[324] 7,000 central offices serving PSAPs * 25 percent lacking fixed generators * 1 percent lacking portable generators * $30,000 per portable generator = $525,000.

[325] Verizon Comments at 12.

[326] *See 911 Reliability NPRM*, 28 FCC Rcd at 3437 ¶ 52.

[327] *Id.*

[328] Verizon Comments at 12.

[329] *See* Verizon Comments at 3 ("Almost all of Verizon's [central offices] are engineered to have on-site, fixed generators with 72-hour fuel reserves as well as battery reserves.").

[330] *See* AT&T Comments at 18.

deploy portable generators in an emergency."[331] Hence, we conclude that the incremental cost to AT&T to comply with our central office backup power certification standard would be modest.

124. We further note that other commenters agree with cost estimates provided in the *NPRM*. CenturyLink, for example, believes the *NPRM's* cost estimate ranges for generator installation are reasonable.[332] NATOA also argues that the Commission's "cost estimate for installing generators at the COs that do not currently have them is reasonable."[333] These comments underscore our conclusion that, particularly given our focus only on the roughly 28 percent of central offices serving PSAPs and the widespread deployment of generator capacity today, as well as the ability of service providers to employ portable generators in accordance with CSRIC best practices, the rules we adopt today are unlikely to result in anything approaching the costs alleged by some service providers.

125. Based on these observations, we conservatively conclude that at most 1 percent of the central offices without fixed generators serving PSAPs do not have portable generators available in the case of an emergency. As stated above, using this assumption and a cost of $30,000 for a portable generator as we did in the *NPRM*, the estimated incremental cost for having portable generators available at all central offices serving PSAPs that lack access to such generators today would be $525,000.[334] Even if the cost of each portable generator is a more conservative $50,000, the total cost would not exceed $875,000.[335]

126. *Battery Testing:* Most service providers claim to test *all* batteries on a routine basis.[336] The cost benefit analysis we included in our *NPRM* assumed that 5 percent were not tested regularly; hence our estimate of testing costs was more conservative in this regard. Regarding testing costs, AT&T comments that "testing costs vary widely based on the size and number of engines and batteries in an office, factors which vary based on the office's size."[337] NATOA argues that our cost analysis is accurate and asserts that regular battery testing is part of a "reasonable baseline of operations and should not be counted as an additional cost."[338] No commenter provided specific battery testing costs that disputed the battery testing costs in our *NPRM* and endorsed by NATOA. The battery testing costs estimated in our *NPRM* applied to just the central offices serving PSAPs are $448,000.

127. *Generator Testing:* Most commenters also state that they routinely test all generators.[339] CenturyLink is the only company which provides cost figures for generator testing. CenturyLink argues that generator testing alone would result in annual costs to industry of $11.8 million, including the cost of repairs.[340] While we agree that Covered 911 Service Providers should make repairs where necessary, we

[331] *See id.* at 8.

[332] *See* CenturyLink Reply Comments at 9.

[333] *See* NATOA Comments at 4-5.

[334] 7,000 central offices serving PSAPs * 25 percent lacking fixed generators * 1 percent lacking portable generators * $30,000 per portable generator = $525,000.

[335] 7,000 central offices serving PSAPs * 25 percent lacking fixed generators * 1 percent lacking portable generators * $50,000 per portable generator = $875,000. As noted above, in the *NPRM* we assumed that 5 percent of the central offices without fixed generators do not have access to a portable generator in the case of an emergency. If we apply the 5-percent figure, the estimated cost would be $2,625,000, which we believe seriously overestimates the cost based on the information that we have received about the existing availability of portable generators.

[336] *See* Verizon Comments at 3,4; AT&T Comments at 17.

[337] *See* AT&T Comments at 19.

[338] NATOA Comments at 5.

[339] *See* Verizon Comments at 3,4; AT&T Comments at 17.

[340] *See* CenturyLink Reply Comments at 10.

do not agree that such costs should be included in routine testing costs. Furthermore, CenturyLink asserts that 10 percent of the central offices do not have generator tests performed. Based on that assumption, CenturyLink calculated that 1,838 central offices would incur costs due to additional generator testing. Because most commenters indicated that they do generator testing wherever they are deployed, we conclude that our original estimate of 5 percent is very conservative for an industry-wide estimate, notwithstanding CenturyLink's experience. Since we only apply our rules to offices that serve PSAPs, this reduces the number of central offices by 72 percent. The number of central offices that would incur costs due to additional generator testing is actually 263, not the 1,838 suggested by CenturyLink.[341] CenturyLink estimated that it takes thirty-five hours to run the yearly tests for a generator.[342] If we assume that CenturyLink is correct about the time it takes to run generator tests, the generator testing costs for 263 offices would be $735,000 for all of the central offices serving PSAPs for which no generator testing was currently done. In addition, CenturyLink pointed out that there are additional fuel costs for running generator tests which we did not include. CenturyLink assumed that tests were run for sixteen hours requiring five gallons of fuel per hour and costing $4 per gallon.[343] If we assume that there are 263 central offices for which these calculations apply we obtain a fuel cost of $84,000. This brings the generator testing cost to $819,000.[344] This is below the $1,176,000 impact nationwide that we estimated in our *NPRM*.[345]

128. *Generator Repaired Soon After It Fails a Test:* In our *NPRM* we included some costs due to commencing the repair of a generator quickly after it failed. There were no comments on the costs, but we believe this estimate to be reasonable based on past experience. If we restrict the backup power rules to central offices serving PSAPs, these costs would be $16,900.

129. *Eliminating Tandem Arrangements:* In our *NPRM*, we targeted generator arrangements where the failure of one generator in a pair of generators would result in a central office losing all backup power. CenturyLink estimated the cost of setting up an automated load shedding arrangement in such locations.[346] But we are not requiring automated load shedding arrangements, and as a result, we do not believe our costs need to be changed. Because we restrict the backup power rules to central offices serving PSAPs, these costs would be only $71,400.

130. *Revised Total Back-up Power Costs:* Combining the costs in the preceding paragraphs, we conclude that the total cost of implementing our certification requirements for backup power in central offices serving PSAPs would be in the range of $1.9 million,[347] which is considerably less than the $11,700,000 we estimated in the *NPRM*. Hence, we find the certification method we adopt today to be cost effective.

[341] 7,000 (central offices serving PSAPs) *.75 (estimated proportion of offices with generators)*.05 (offices where testing is not performed) = 263.

[342] *See* CenturyLink Reply Comments at 10.

[343] *See id.*

[344] In our *NPRM* we assumed that it took sixteen hours a year to test each generator. Our cost using this figure for testing generators in 263 offices would be $336,000. In addition, we estimated no fuel costs. By adopting CenturyLink's figures, this raises the cost to $819,000.

[345] *See 911 Reliability NPRM*, 28 FCC Rcd at 3437-38 ¶ 54 (estimating a maximum of $882,000 for monthly generator testing and $294,000 for annual testing, for a total of $1,176,000).

[346] *See* CenturyLink Reply Comments at 10.

[347] $525,000 for portable generators + $819,000 for generator testing + $448,000 for battery testing + $16,900 for expedited generator repairs + $71,400 to remediate interdependent generators = $1,880,300.

3. Network Monitoring

131. In light of the importance of accurate situational awareness during any network outage, the findings of the *Derecho Report*, and the comments in the record, we also require Covered 911 Service Providers to certify annually whether they have, within the past year: (1) audited the physical diversity of the aggregation points that they use to gather network monitoring data in each 911 service area[348] and the network monitoring links between such aggregation points and their NOC(s); and (2) implemented physically diverse aggregation points for network monitoring data in each 911 service area and physically diverse links from such aggregation points to at least one NOC or, in light of the required audits, taken specific alternative measures reasonably sufficient to mitigate the risk of insufficient physical diversity. They may also certify that they believe this element of the certification is not applicable to their network, although they must explain why it is not applicable. Covered 911 Service Providers also must retain records of their network monitoring routes and capabilities for confidential review by the Commission, upon request, for two years.

132. For purposes of the certification, network monitoring links transmit data about failed or degraded network equipment and facilities from monitoring points within the network to a NOC or other location where the data are analyzed and decisions made about corrective action. Links from multiple individual monitoring points may be routed through and aggregated onto common transport facilities at one or more hubs in each service area for distribution to remote NOCs, in which case those hubs are described as aggregation points for network monitoring data. "Physical diversity" applied to aggregation points refers to aggregation points that are not physically co-located.

133. During the derecho, the network monitoring capabilities of the two primary 911 service providers involved were non-operative within the area of the storm, depriving them of visibility into the status of their networks and complicating their recovery efforts. In both instances, a widespread loss of network monitoring capabilities could be attributed to a single point of failure, such as one central office collecting telemetry data for dozens of facilities in northern Virginia.[349] Large carriers that serve multiple states or regions typically use one or more central offices as hubs to gather telemetry data from multiple end points in each service area (*e.g.*, smaller offices, selective routers, remote switches, etc.) and transmit that aggregated information to a NOC for remote monitoring and analysis. Diversity of regional aggregation points for the collection of monitoring data, including the diversity of the facilities that connect those aggregation points to NOCs, is vital to communications reliability because service providers cannot diagnose and repair problems if they are unaware that they exist.

134. Two CSRIC best practices address circuit diversity and network monitoring in general terms. One of these best practices calls for network diversity audits on critical circuits,[350] and another states that network operators "should monitor their network to enable quick response to network issues."[351] At a minimum, the failures documented in the *Derecho Report* confirm that it is a sound engineering practice to design network monitoring architectures with visibility into the network through physically diverse aggregation points and monitoring links interconnecting to NOCs to help avoid single points of failure. Accordingly, we adopt certification requirements that refine these CSRIC best practices,

[348] Service providers typically collect network monitoring data through geographically distributed aggregation points, which may correspond to major metropolitan areas but may also vary in size and location by service provider. We intend the certification obligation in this section to ensure that large service providers have diverse access to monitoring data in each of the major service areas in which they are the major provider of 911 service, *i.e.*, operate the selective routers or equivalent, but not necessarily to every end point in their networks.

[349] *See 911 Reliability NPRM*, 28 FCC Rcd at 3439 ¶ 59.

[350] *See* CSRIC Best Practice 8-7-0532, *available at* https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=8-7-0532.

[351] CSRIC Best Practice 8-7-0401, *available at* https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=8-7-0401.

and provide additional guidance to Covered 911 Service Providers regarding reasonable alternative measures with respect to network monitoring.

135. Commenters generally agree that network monitoring is vital to the reliability of 911 services, although RLECs and other small entities assert that NOCs and regional aggregation points are "predominately [a] large carrier concept," and that diverse access may not be feasible when there is only one practical route between remote facilities.[352] Other commenters, however, observe that alternate transmission technologies, like satellite, can be used to achieve physical diversity between aggregation points and NOCs when wired paths are unavailable.[353] EchoStar, for example, notes that emergency authorities have used broadband satellite links to provide backup communications when their terrestrial networks fail.[354] We note that methods like this, where reliable, would qualify as reasonable alternative measures to help ensure 911 reliability where diverse aggregation points or NOC interconnection facilities are not feasible.

136. Despite the claims of many commenters that they have already taken steps to ensure the resiliency of network monitoring systems, the vital importance of accurate situational awareness during disasters and other emergencies causes us to conclude that Commission oversight is needed to ensure these improvements occur consistently nationwide. AT&T, for one, describes a program to route network monitoring traffic on a more resilient IP-enabled network and eliminating, over time, single points of failure in its monitoring network.[355] Frontier has "updated its corporate network diversity, providing protection to the management network that the Network Operations Center (NOC) uses to access equipment in central offices. This process is ongoing."[356] Verizon is "rebuilding its telemetry system to provide more diverse connections and alternate [backup] locations, in the event of a problem at a location where telemetry information is aggregated."[357] Verizon also is migrating telemetry traffic across its network to a more robust IP-based network and implementing a procedure to prevent circuit rearrangements that can remove circuits from a diverse configuration.[358] We note that all of these measures are entirely consistent with the certification standards we adopt today.

137. *Corrective Measures.* Recognizing that circumstances are likely to exist in real-world networks that prevent the achievement of complete physical diversity and diverse aggregation points for network monitoring data, we agree with ATIS that service providers should "retain the flexibility to implement diversity and the migration of telemetry to the IP network as appropriate for their network evolution, management, and monitoring."[359] Our certification approach provides Covered 911 Service Providers with the flexibility to compensate for an inability to conform to our certification standard by employing appropriate alternative measures to promote reliable and resilient network monitoring where diverse aggregation points or monitoring links may not be feasible.

138. *Cost Effectiveness.* No respondents claim that our proposal is not cost effective. On the contrary, both AT&T and Verizon claim that our requirement of diversity in network monitoring facilities

[352] *See* Western Telecommunications Alliance Comments at 10 (stating that "for most WTA members and other RLECs their 'NOC' is their central office technician and his various wireline and wireless phones"); NTCA Comments at 6.

[353] *See* EchoStar/Hughes Ex Parte Notice at 2 (July 2, 2013) ("[A]s the Commission considers path diversity, it should recognize satellite as a valued, reliable option for route diversity.").

[354] *Id.*

[355] *See* AT&T Comments at 20-21.

[356] *See* Frontier Comments at 3.

[357] *See* Verizon Comments at 6.

[358] *See id.*

[359] *See* ATIS Comments at 11.

is unnecessary because they already satisfy the requirement[360] or are in the process of implementing it.[361] As mentioned previously, while many of the measures described in our certification may now be in place, the seriousness of the lapses revealed by the derecho calls upon us to exercise further oversight to ensure that these standards continue to be met. In our *NPRM*, we assumed that 75 percent of the major metropolitan areas lacked diverse monitoring links.[362] Based on the preceding information from AT&T and Verizon, this 75-percent figure is probably too high. If we reduce this to a more realistic 25 percent, we calculate the costs to be $732,000,[363] as opposed to $2,196,000 that we assumed in our *NPRM*.[364] In the absence of more detailed cost estimates from commenters, we find that the certification approach we adopt today is cost effective because it uses standards that are already widely in use by communications providers and includes flexibility to allow communications providers to address circumstances where the standards cannot be feasibly implemented.

E. PSAP Outage Notification

139. To ensure that PSAPs receive timely and actionable notification of 911 outages, we amend section 4.9[365] of our rules. The Commission's existing outage-reporting rules recognized that PSAPs must be notified when communications outages affect 911 service, but they only required notification "as soon as possible" with "all available information that may be useful."[366] The derecho revealed that many PSAPs' efforts to restore service were complicated by inadequate information and otherwise ineffective communication by service providers.[367] Multiple PSAPs stated that they contacted their 911 service provider to report a loss of service before being contacted by the provider, and others received notification in the form of "cryptic" e-mails that referenced problems in one central office but did not specify all of the jurisdictions affected. Inadequate information from service providers during the derecho also led some PSAPs to activate ineffective reroutes, or to keep a reroute active even though service had been restored on the original route.

140. Under the amended rule, Covered 911 Service Providers must notify PSAPs of outages potentially affecting 911 service to that PSAP within thirty minutes of discovering the outage and provide contact information such as a name, telephone number, and e-mail for follow-up. As Fairfax County observes, this initial notification should be based on the "best available information," but the unavailability of any piece of information should not delay a service provider's initial contact with an affected PSAP.[368] Unlike for purposes of outage reporting in NORS, service providers must notify PSAPs of 911 outages *upon discovering the outage*, not upon determining that the outage is NORS-reportable.[369]

141. Whenever additional material information becomes available, but no later than two hours after the initial contact, the Covered 911 Service Provider must communicate additional detail to the PSAP, including the nature of the outage, its best-known cause, the geographic scope of the outage, and

[360] *See* AT&T Comments at 19-21.

[361] *See* Verizon Comments at 6.

[362] *See 911 Reliability NPRM*, 28 FCC Rcd at 3441 ¶ 66.

[363] 366 metropolitan areas in United States * 25 percent lacking diverse monitoring links * 100 hours to add each diverse access point * $80 per hour = $732,000.

[364] *See 911 Reliability NPRM*, 28 FCC Rcd at 3441 ¶ 66.

[365] 47 C.F.R. § 4.9.

[366] *See id.*

[367] *See 911 Reliability NPRM*, 28 FCC Rcd at 3441-43 ¶¶ 67-69.

[368] *See* Fairfax County Comments at 10.

[369] *See* NENA Ex Parte Notice (May 25, 2013).

the estimated time for repairs.[370] Although the *911 Reliability NPRM* proposed requiring additional details such as the estimated number of users affected, actions being taken by the service provider to address the outage, and recommended actions the impacted facility should take to minimize disruption of service,[371] commenters disagree whether this information is reasonably available to service providers or useful to PSAPs during a service outage.[372] Accordingly, while we decline to specifically require this information in all outage notifications, we encourage service providers to include these and other details that may be useful to affected PSAPs as they become available.

142. The *911 Reliability NPRM* proposed requiring service providers to notify PSAPs of 911 outages "immediately by telephone and in writing via electronic means."[373] The rules we adopt today provide a more objective basis for enforcement. APCO, for example, notes that "the term 'immediately' could be open to disputed interpretation" and suggests that notification should be provided "immediately, within no more than 15 minutes of the service provider becoming aware of the outage."[374] Other public-safety commenters recommend initial notification "within 15 to 30 minutes (maximum) of the discovery of an outage,"[375] or "within one hour of discovery."[376] We believe the thirty-minute limit adopted here strikes an appropriate balance between these comments and service providers' need for time to gather information.

143. Generally, commenters note that there will likely be a tradeoff between the time allowed for notification and the amount and accuracy of information available.[377] Fairfax County observes that a requirement to communicate specific information such as the nature and location of the outage should not prevent service providers from notifying PSAPs immediately with a "broad-brush picture of the situation" and following up with additional information as it becomes available.[378] We agree with this approach and believe it accounts for the concerns of PSAPs and service providers.

144. Commenters also addressed acceptable methods of outage notification. Some suggest that notification "by telephone and in writing" should not preclude PSAPs and service providers from agreeing on alternative methods of communication if they prefer.[379] APCO comments that "the method of notification should include electronic communication and positive, verified human contact with an on-

[370] *See* NENA Comments at 13 ("In particular, NENA believes that information about the geographic scope of an outage, its best-known cause, and an estimate of time to repair (or, if none is available, a notation as to when it can be expected) will greatly aid public safety agencies in crafting public messaging and tactical response plans during outages.").

[371] *See 911 Reliability NPRM*, 28 FCC Rcd at 3443 ¶ 70.

[372] *See* CenturyLink Reply Comments at 14 (arguing that service providers should not be required to recommend actions the impacted facility should take to minimize disruption of services because such decisions should be left to PSAPs); AT&T Comments at 23 (arguing that a requirement to notify PSAPs immediately could result in dissemination of "incomplete and inaccurate information"); Verizon Comments at 20 (arguing that specific information about outages should be required only "to the extent it is reasonably available to the provider").

[373] *See 911 Reliability NPRM*, 28 FCC Rcd at 3443 ¶ 70.

[374] APCO Comments at 3.

[375] NENA Ex Parte Notice at 1 (May 25, 2013).

[376] City of New York Reply Comments at 2.

[377] *See* Verizon Comments at 21 (recommending that specific information be required only "to the extent it is reasonably available to the provider").

[378] *See* Fairfax County Comments at 8-9.

[379] *See* Verizon Comments at 22 (discussing option of conference call to multiple PSAPs affected by an outage); AT&T Comments at 22 (arguing that "new rules may degrade the quality of completeness of information already provided to PSAPs as a result of individualized discussions").

duty PSAP supervisor."[380] Similarly, "NENA believes that both telephone and email notification of outages should be required offerings, but also believes that carriers, SSPs, and 911 authorities should have the flexibility to agree to other primary means of notification that might better meet 911 authorities' requirements."[381] We agree and note that our amendments do not preclude service providers and PSAPs from establishing additional means of communication during an outage so long as they are mutually agreed upon in advance so that PSAPs can plan accordingly.

145. One commenter argues that some PSAPs may not want to receive outage notifications, and the Commission should provide an "opt-out mechanism" for those PSAPs.[382] This appears to be based on the argument that "a PSAP may not have an administrative presence on a full-time (24/7) basis" and that "911 service providers should also have flexibility in determining specific information that is desired or needed by the individual PSAPs."[383] We decline to adopt any such language. Our goal is to ensure that PSAPs receive timely and actionable notification of 911 outages by establishing minimum criteria by which 911 service providers must abide. The overwhelming majority of comments indicate that PSAPs desire to receive as much information as possible about such outages, without the need for an opt-out mechanism.[384]

146. Some commenters argue that more stringent PSAP notification requirements would increase costs to service providers and divert resources away from more productive efforts to restore services.[385] We disagree, and stress that we do not seek to replace the existing scheme with a new, more onerous one, but rather to clarify the timing and notification content with which certain service providers subject to section 4.9 must already comply. Experience from the derecho indicated that some service providers were not complying with the most basic portion of the rules, *i.e.*, the obligation to actually contact the PSAP. We trust that our action today will provide more guidance on expectations for providers, and increased compliance with the outage notification rules. Our goal is certainly not to substantially increase the burden on service providers; nor is it to divert them from performing what is ultimately the most important task – restoring emergency communications services.

147. These amendments to section 4.9 will extend to all Covered 911 Service Providers, as defined in this *Report and Order*,[386] regardless of the technology they employ. One commenter urges us to amend the outage-notification rules covering a broader range of communications providers, including those that originate 911 calls.[387] In light of the limited focus of this proceeding, however, we conclude that the specific obligations of the amended rules should apply only to Covered 911 Service Providers, which are the entities most likely to experience reportable outages affecting 911 service. We defer for

[380] APCO Comments at 4.

[381] NENA Comments at 13.

[382] ATIS Comments at 12.

[383] *Id.*

[384] *See* Fairfax County Comments at 8 ("Communication to the PSAPs is paramount, as the public and elected officials turn to the PSAPs for immediate information on how best to respond to an emergency.").

[385] *See, e.g.*, Blooston Rural Carriers Comments at 6 ("Requiring rural carriers to spend an ever-increasing amount of time and money on gathering data and filing reports with the Commission diverts attention from operating and monitoring the network."); American Cable Association Comments at 13 ("[I]t is particularly important for the Commission to adopt reasonable standards regarding the scope of the information that is required to be reported to the PSAPs.").

[386] *See* ¶ 36, *supra*.

[387] *See* APCO Ex Parte Notice (June 17, 2013) (arguing that "the definition of '911 service provider' for purposes of outage notification requirements should be sufficiently broad to include any facilities or services involved in the initiation, transport, or delivery of a 911 call," including wireline, wireless, and interconnected VoIP providers and transport systems associated with the delivery of call and caller information).

future consideration whether other entities currently subject to PSAP notification requirements (*i.e.*, cable, satellite, wireless, wireline, and interconnected VoIP providers) should be subject to more specific obligations based on the functions they provide in 911 networks.[388]

F. Legal Authority

148. The *911 Reliability NPRM* sought comment on the potential sources of legal authority for Commission action to promote the reliability and resiliency of communications infrastructure that is essential for 911 service. Beyond the Commission's general mandate to "promot[e] the safety of life and property through the use of wire and radio communications,"[389] Congress has delegated to the Commission specific responsibilities to "designate 911 as the universal emergency telephone number for reporting an emergency to appropriate authorities and requesting assistance."[390] Our efforts to ensure that such reports and requests for assistance can reliably be transmitted are "necessary in the public interest to carry out" this provision of the Communications Act.[391] Further, there has been judicial recognition of "[t]he broad public safety and 911 authority Congress has granted the FCC"[392] through legislation such as the Wireless Communications and Public Safety Act of 1999, the NET 911 Improvement Act of 2008, and the Twenty-First Century Communications and Video Accessibility Act of 2010.[393]

149. To the extent that 911 service providers provide interstate common carrier service, the Communications Act also provides that their "practices" must be "just and reasonable,"[394] and that a common carrier must "provide itself with adequate facilities for the expeditious and efficient performance of its service as a common carrier."[395] Because the rules we adopt today are not directed at wireless providers, insofar as that they do not currently provide 911 service directly to PSAPs, we need not address here the potential basis for promulgating these rules under the Commission's Title III authority to "[p]rescribe the nature of the service to be rendered" [396] by wireless providers, and more generally "to manage spectrum . . . in the public interest."[397]

150. In 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 foregoing statutory authority.[398] Although few commenters question the Commission's

---

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

[389] 47 U.S.C. § 151.

[390] 47 U.S.C. § 251(e)(3).

[391] 47 U.S.C. § 201(b). *See also* IP-Enabled Services; E911 Requirements for IP-Enabled Service Providers, *First Report and Order and Notice of Proposed Rulemaking*, 20 FCC Rcd 10245 ¶ 34 (2005), *aff'd sub nom. Nuvio Corp. v. FCC*, 473 F.3d 302 (D.C. Cir. 2007) (*VoIP 911 Order*) (recognizing plenary authority under Section 251(e) to require "network changes" needed to ensure safe, reliable, nationwide 911 system).

[392] *Nuvio Corp. v. FCC*, 473 F.3d 302, 311 (D.C. Cir. 2007) (Kavanaugh, J., concurring).

[393] *See 911 Reliability NPRM*, 28 FCC Rcd at 3444-45 ¶ 76.

[394] 47 U.S.C. § 201(b).

[395] 47 U.S.C. § 214(d).

[396] 47 U.S.C. § 303(b).

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

[398] Although ensuring reliable 911 service lies clearly within the Commission's statutory authority under specific 911 statutes as well as the foregoing specific grants of authority under Title II and Title III, our prior experience and the record of this proceeding demonstrate for the reasons stated above that the rules we adopt for ensuring reliable 911 service are also both within our jurisdictional grant under Title I and "reasonably ancillary to the Commission's effective performance of [these] statutorily mandated responsibilities." *American Library Ass'n v. FCC*, 406 F.3d

(continued….)

legal authority over 911 communications,[399] one suggests that the Commission lacks authority to adopt 911 reliability rules because it asserts that 911 calls are purely intrastate. Thus, the commenter argues, the Commission "should at most adopt or endorse *recommended* best practices for state and/or local authorities to adopt."[400] The Commission has rejected similar arguments in the past, however, relying on the 911 statutes enacted by Congress as an endorsement of the Commission's role in this area.[401] Our plenary authority over 911 numbering, for example, was enacted pursuant to the Wireless Communications and Public Safety Act of 1999, whose express purpose is "to encourage and facilitate the prompt deployment throughout the United States of a seamless, ubiquitous, and *reliable* end-to-end infrastructure for communications, including wireless communications, to meet the Nation's public safety and other communications needs."[402] Commenters also describe the interstate nature of at least some portions of 911 network architecture.[403] Moreover, the state public utilities commissions filing comments in this proceeding have uniformly endorsed our proposals,[404] which do not extend to matters of state or local jurisdiction such as tariff conditions and the internal operation of PSAPs. Indeed, as noted above, we have specifically declined to include PSAPs within our definition of Covered 911 Service Providers or otherwise to regulate the reliability of their own internal operations. To the extent that commenters express concern about the appropriate line between federal and state authority with respect to 911 service,

(Continued from previous page)
689, 691-92 (D.C. Cir. 2005). *See also* 47 U.S.C. § 154(i); *United States v. Southwestern Cable Co.*, 392 U.S. 157, 178 (1968); Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications, *Report and Order*, 28 FCC Rcd 7556 ¶¶ 128-40 (2013).

[399] *See e.g.* Verizon Reply at 7 (arguing that the Commission is looking only at the reliability and resiliency 'of the 911 system'" and cautioning against adopting proposals that would "significantly broaden [the Commission's] rulemaking into providers' backup power practices…").

[400] *See* Boulder Regional Emergency Telephone Authority (BRETSA) Comments at 2 (emphasis in original).

[401] *See VoIP 911 Order*, 20 FCC Rcd at 10263 ¶¶ 29-30 n.95 (2005), *aff'd sub nom. Nuvio Corp. v. FCC*, 473 F.3d 302 (D.C. Cir. 2007) ("[W]hile we acknowledge that there are generally intrastate components to interconnected VoIP service and E911 service, we reject any argument that 911/E911 services are purely intrastate and therefore the Commission has no jurisdiction in this area. The Commission has long maintained a federal role in wireline and wireless 911/E911 issues."). *See also* Petition for Declaratory Ruling That Pulver.com's Free World Dialup Is Neither Telecommunications Nor a Telecommunications Service, *Memorandum Opinion and Order*, 19 FCC Rcd 3307 ¶ 21 (2004).

[402] Pub. L. No. 106-81, 113 Stat. 1286, § 2(b) (1999) (emphasis added). Congress established our plenary jurisdiction over 911 numbering as a subsection of Section 251(e) of the Communications Act. While this provision of the Act grants the Commission the authority to "delegat[e] to State commissions or other entities all or any portion of such jurisdiction," 47 U.S.C. § 251(e)(1), the Commission has retained "authority to set policy with respect to all facets of numbering administration in the United States." Numbering Policies for Modern Communications, *Notice of Proposed Rulemaking, Order and Notice of Inquiry*, 28 FCC Rcd 5842 ¶ 84 (2013); *VoIP 911 Order*, 20 FCC Rcd at 10265 n.110. The Commission has found that "Section 2(b) [of the Act] . . . imposes no limitation upon the Commission's exclusive authority under section 251(e) to perform ongoing numbering administration functions." Implementation of the Local Competition Provisions of the Telecommunications Act of 1996, *Third Order on Reconsideration of Second Report and Order and Memorandum Opinion and Order*, 14 FCC Rcd 17964 ¶ 36 (1999), *aff'd sub nom. New York and Public Service Comm'n of New York v. FCC*, 267 F.3d 91, 102 (2d Cir. 2001).

[403] *See* NENA Reply Comments at 2 n.5 ("Many database links, for example, now connect with widely dispersed data centers in Colorado, Florida, Maryland, Washington, etc., regardless of where a 9-1-1 call originates or terminates."); Pennsylvania PUC Comments at 10 n.8 (citing 911 network functionalities, including delivery of ALI, across state boundaries); ¶¶ 7-9 *supra*.

[404] *See* California PUC Comments at 4, 8 (urging FCC to adopt certification scheme and backup power requirements); Pennsylvania PUC Comments at 4 (urging imposition of best practices as federal regulatory minimums); Virginia State Corporation Commission Comments at 9 ("We encourage and support the FCC's efforts in this proceeding to ensure the reliability of 911 to all citizens in Virginia and the nation").

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. The rules we adopt today are not intended to preempt state and local actions so long as they do not operate to frustrate the implementation of the Commission rules adopted here. We do not believe it is appropriate or feasible, however, to make any specific determinations about preemption, including whether supplemental state or local requirements are consistent with the balancing of costs and benefits reflected in our new rules, without an actual – not hypothetical – case of state or local action in this area. The question of whether such action would frustrate the implementation of the Commission's federal regulatory framework would turn on the individual circumstances of each case. We do observe, however, that the rules adopted here may obviate the need for state and local jurisdictions to promulgate their own requirements, thereby reducing the prospect of disparate regulatory schemes and simplifying the regulatory burdens on service providers.[405]

G. Confidentiality

151. We have long recognized that certain information about communications networks may be competitively sensitive or reveal vulnerabilities to individuals or organizations with hostile intent, and should therefore generally be treated as confidential.[406] We also have observed, however, that "not all information needs to be protected" and that allegations of competitive harm "must flow from affirmative use of the information by competitors and not consist solely of injuries that flow from customer disgruntlement or public embarrassment."[407]

152. The *911 Reliability NPRM* sought comment on whether reliability information submitted by 911 service providers should be made publicly available or presumed confidential.[408] The *NPRM* also inquired whether such information "should be shared within the PSAP community, or made accessible to 911 industry associations (*e.g.*, APCO, NENA)," as was the case with previous reports on redundancy and resiliency of 911 networks under section 12.3 of our rules.[409] Additionally, the *NPRM* asked whether reliability information should be shared with state public utilities commissions.[410]

153. Most commenters agree that proprietary 911 network information is potentially sensitive and should not be disclosed to the general public, although they disagree about the scope of disclosure to other entities. Verizon, for example, states that "[w]hile the CPNI certification is filed in a public docket, a 911 resiliency certification should be afforded full confidentiality protection in light of the sensitive nature of the information disclosed."[411] ATIS contends that certification results should be withheld from

[405] For these reasons, we decline to address here BRETSA's October 25, 2012, Petition for Declaratory Ruling requesting the Commission to "clarify the extent to which it has preempted state regulation of 911 and SSP service." *See* BRETSA Comments at 2-3. Moreover, consideration of the petition here is inappropriate because it raises issues beyond the scope of this proceeding. We also defer BRETSA's arguments regarding service provider liability under PS Docket No. 11-153 for later consideration in that docket.

[406] *See Part 4 Order*, 19 FCC Rcd at 16855 ¶ 45. *See also* Alaska Communications Systems Comments at 9 (noting that "significant disclosure of the design and implementation process for 911 capability itself could introduce security threats").

[407] *Part 4 Order* at 16848 ¶ 31, 16854 ¶ 43.

[408] *See 911 Reliability NPRM*, 28 FCC Rcd at 3432, 3436 ¶¶ 39, 47.

[409] *See* FCC's Public Safety and Homeland Security Bureau Announces the Activation of the E911 Architecture Information System, *Public Notice*, DA 08-2263, 23 FCC Rcd 14757 (PSHSB 2008); In the Matter of Implementation of Section 12.3 of the Commission's Rules, DA 09-1077, *Protective Order*, 24 FCC Rcd 5657 (2009) (noting that the Commission would share reports with certain public safety organizations subject to a presumption of confidentiality).

[410] *See 911 Reliability NPRM*, 28 FCC Rcd at 3432 ¶ 39.

[411] Verizon Comments at 13 n.21.

the states unless proper safeguards are in place.[412] Similarly, CenturyLink comments that "[t]o the extent any [circuit] audits are mandated, those audits should be treated as proprietary business information that is presumed confidential."[413] CenturyLink, however, generally agrees that PSAPs should have access to relevant information in at least a summary form.[414]

154. Public safety and state government commenters recognize the sensitivity of this information, but argue for at least limited access to information. Fairfax County specifically argues that "detailed information from [circuit] audits needs to be shared with the PSAP to which the information relates," though it agrees that "such detailed network configuration information should be required to be treated by all parties as sensitive and confidential information."[415] State regulators in California and Pennsylvania request access to information collected through the Commission's certification process.[416]

155. It is clear that the information at issue in the certifications holds great value for public safety and state authorities, but we have consistently recognized the sensitivity of this type of information and the need to protect it from broad disclosure.[417] On balance, we conclude that some components of annual 911 reliability certifications are likely to raise genuine public safety and competitive concerns, while other portions of the certification will not and may be of legitimate interest to the public. For example, we perceive little threat to public safety or competition in the mere fact of whether a Covered 911 Service Provider has filed a certification, or whether a service provider answers in the affirmative or negative to each element of the certification. Thus, we would *not* consider confidential a service provider's responses on the face of the form with respect to whether it adheres to certification elements or relies on alternative measures to satisfy other elements of the certification.

156. We recognize, however, that confidentiality concerns increase significantly if a certification includes proprietary information about a service provider's specific network architecture or operations on less than an aggregated basis. Accordingly, as with our mandatory outage-reporting requirements,[418] we will treat as presumptively confidential and exempt from routine public disclosure under the Freedom of Information Act (FOIA): (1) descriptions and documentation of alternative measures to mitigate the risks of nonconformance with certification standards; (2) information detailing specific corrective actions taken; and (3) supplemental information requested by the Commission or Bureau with respect to a certification. Examples of information we will treat as presumptively confidential include circuit routes and diagrams, maintenance records, internal policies and procedures, and outage data.[419]

---

[412] *See* ATIS Comments at 10.

[413] CenturyLink Reply Comments at 3.

[414] *See id.* at 3 ("CenturyLink supports sharing summary information with its PSAP customers that is directly applicable to them.").

[415] Fairfax County Comments at 4-5.

[416] California PUC Comments at 6; Pennsylvania PUC Comments at 4.

[417] *See Part 4 Order*, 19 FCC Rcd at 16855 ¶ 45.

[418] *See Part 4 Order* at 16852-55 ¶¶ 40-46; MSNBC Interactive News, LLC, *Memorandum Opinion and Order*, 23 FCC Rcd 14518 (2008). *See also* 47 C.F.R. §§ 0.457(d)(1)(vi), 4.2.

[419] Our decision here does not extend to whether states may have access to NORS data. In 2009, the Commission received a petition for rulemaking from the California PUC to allow states direct access to NORS outage reporting data. *See* Petition of the California Public Utilities Commission and the People of the State of California for Rulemaking on States' Access to the Network Outage Reporting System (NORS) Database and a Ruling Granting California Access to NORS, ET Docket No. 04-35, *Petition for Rulemaking* (filed Nov. 12, 2009). The petition remains pending, and while it involves many of the issues raised here with respect to sharing of certification data, we agree with Verizon to defer a decision about sharing certification data with state regulators until the issue is resolved in the context of outage reporting. *See* Verizon Comments at 9.

157. We also recognize that PSAPs and state 911 authorities have a strong interest in obtaining relevant information about the reliability and resiliency of their 911 service. As NENA states, PSAPs may be in the best position to use this information to prompt 911 service providers to make specific reliability improvements in their networks, but they may not otherwise be able to negotiate reliable access to this information through their contracts or tariffs.[420] As noted, Fairfax County argues for disclosure to PSAPs of detailed information on circuit audits.[421] The record in this proceeding supports allowing PSAPs and, as relevant, state 911 authorities, access to potentially sensitive information on the circuit routes to the PSAP. No PSAPs have identified any other proprietary information that they believe to be important in assessing reliability of their service, and accordingly, we have no reason to address here the need for disclosure of additional information to PSAPs and/or state 911 authorities.

158. To this end, we expect that a Covered 911 Service Provider will, at the request of the PSAP (or state 911 authority, as relevant), enter into discussions concerning the content of the provider's 911 circuit auditing certification with respect to the PSAP. In light of the wide variety of circumstances involved in how PSAPs nationwide purchase 911 service, we decline to require specific disclosure by rule, preferring to allow parties to negotiate reasonable and appropriate terms for assuring protection of proprietary information. We make clear, however, that Covered 911 Service Providers should respond promptly to a PSAP request in this area and reiterate our belief that PSAPs should have access to the details of circuit-auditing certifications, as long as the sensitive and proprietary nature of the information can be maintained.

H. Review and Sunset of Rules

159. The Commission will review the rules adopted in this *Report and Order* in five years to determine whether they are still technologically appropriate and both adequate and necessary to ensure reliability and resiliency of 911 networks.[422] Review of the rules will also include consideration of whether they 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. Factors for consideration will include outage reporting trends, adoption of NG911 capabilities on a nationwide basis, and whether the certification approach has yielded the necessary level of compliance. If, after review, the Commission determines that some or all of these rules are no longer effective in promoting 911 reliability, we will establish an appropriate sunset date for those portions of the rules that are no longer necessary. At the same time, a lack of compliance with certification requirements or persistence of preventable 911 outages could indicate a need for broader or more rigorous rules.

160. As noted in the *NPRM*, the transition to NG911 will likely drive improvements in network reliability and resiliency compared to the current circuit-switched system because of the inherently diverse nature of IP networks. Network architecture, backup power, and network monitoring technologies may also evolve as new entities begin providing NG911 services. Consequently, Commission actions to promote reliability of current 911 infrastructure may no longer be necessary in light of future improvements to the network. If these improvements are not realized as expected, however, additional Commission action may be warranted.

161. Few commenters have directly addressed the issue of a review or sunset period; however, there is broad agreement that any rules adopted in this proceeding should account for the transition to

[420] *See* NENA Ex Parte Notice at 2 (June 3, 2013) (expressing concern that "some carriers have chosen to exploit their market position to deny public safety agencies and their representatives the very data they insist is lacking in NENA's and others' presentations to the FCC" regarding reliability and redundancy of 911 networks).

[421] *See* Fairfax County Comments at 4-5.

[422] We intend this review to extend to the annual 911 reliability certification and associated elements adopted herein. Because the record reflects a need for detailed outage notification to PSAPs both before and after the adoption of NG911, we do not contemplate a review or sunset of the amendments to section 4.9.

NG911 without impeding that transition through regulatory obligations based on legacy technologies.[423] As noted above, the record also indicates that certain certification requirements related to circuit auditing and physical diversity of 911 circuits may be particularly important to today's circuit-switched networks, while IP-based NG911 networks are likely to be more inherently diverse and resilient. We may therefore revisit factors such as the timing of circuit audits and the auditing practices incorporated in the certification as appropriate based on new technologies.

162. While we commit to a review of these rules after five years, we decline to set a specific sunset date or triggering event because there are still too many uncertainties about the timeline for widespread adoption of NG911 and the effect of new technologies on the need for 911 reliability rules. A five-year review period will allow for meaningful technological progress in the deployment of NG911 without tying the Commission and various parties in the 911 community to long-term rules based on current technologies. Although ubiquitous adoption of NG911 could obviate the need for some of these rules, we believe it would be inappropriate to adopt a complete sunset while significant portions of the nation may still rely on legacy infrastructure.[424]

I. Authority Delegated to PSHSB

163. We delegate authority to PSHSB to implement the rules adopted in this *Report and Order*, consistent with the Administrative Procedure Act and relevant portions of the Communications Act. Specifically, we direct the Bureau to develop such forms and procedures as may be required to collect and process certifications, and we delegate authority to the Bureau to periodically update those forms and procedures as necessary, subject to Paperwork Reduction Act requirements. Through its experience with electronic outage reports in NORS and DIRS, the Bureau has developed expertise with outage reports and trends that will be useful when reviewing such certifications and identifying issues for follow-up with service providers. We also delegate authority to the Bureau to order appropriate remedial actions on a case-by-case basis where 911 reliability certifications indicate such actions are necessary to protect public safety and consistent with the guidelines set forth in this *Report and Order*.

IV. PROCEDURAL MATTERS

A. Final Regulatory Flexibility Act Analysis

164. Pursuant to the Regulatory Flexibility Act of 1980, as amended,[425] the Commission's Final Regulatory Flexibility Analysis (FRFA) relating to this Report and Order is attached as Appendix C.

B. Paperwork Reduction Act Analysis

165. This document contains new information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. It will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies are invited to comment on the new or modified information collection requirements adopted in this *Report and Order*.

166. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198,[426] we previously sought specific comment on how the Commission might further

[423] *See* NENA Comments at 14 (noting generally that "NG911 systems will require somewhat different reliability rules").

[424] *See* NATOA Comments at 3 ("While we welcome the opportunities that new technologies bring to public safety communications capabilities, we emphasize that as new technologies evolve, the reliability of the legacy network remains a critical asset in stable emergency communications.").

[425] *See* 5 U.S.C. § 604.

[426] *See* 44 U.S.C. 3506(c)(4).

reduce the information collection burden for small business concerns with fewer than 25 employees. In this present document, we have assessed the effects of 911 reliability certification rules on small business concerns, and find that the rules adopted here minimize the information collection burden on such businesses by allowing them to describe reasonable alternative measures in lieu of specified certification elements or to explain why a certification element is not applicable to their networks. This flexible approach allows entities with limited resources to comply with our rules in a cost-effective manner.

C. Congressional Review Act

167. The Commission will send a copy of this *Report and Order* to Congress and the Government Accountability Office pursuant to the Congressional Review Act.[427]

V. ORDERING CLAUSES

168. Accordingly, IT IS ORDERED pursuant to sections 1, 4(i), 4(j), 4(o), 201(b), 214(d), 218, 251(e)(3), 301, 303(b), 303(g), 303(r), 307, 309(a), 316, 332, 403, 615a-1, and 615c of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154(i)-(j) & (o), 201(b), 214(d), 218, 251(e)(3),301, 303(b), 303(g), 303(r), 307, 309(a), 316, 332, 403, 615a-1, and 615c, that this *Report and Order* in PS Docket No. 13-75 and PS Docket No. 11-60 IS ADOPTED.

169. IT IS FURTHER ORDERED that Parts 0, 4, and 12 of the Commission's Rules, 47 C.F.R. Parts 0, 4, and 12, ARE AMENDED as specified in Appendix B, effective 30 days after publication in the *Federal Register,* except that those amendments which contain new or modified information collection requirements that require approval by the Office of Management and Budget under the Paperwork Reduction Act WILL BECOME EFFECTIVE after the Commission publishes a notice in the *Federal Register* announcing such approval and the relevant effective date.

170. IT IS FURTHER ORDERED that the Final Regulatory Flexibility Analysis in Appendix C hereto IS ADOPTED.

171. IT IS FURTHER ORDERED that, pursuant to Section 801(a)(1)(A) of the Congressional Review Act, 5 U.S.C. § 801(a)(1)(A), the Commission SHALL SEND a copy of this Report and Order to Congress and to the Government Accountability Office.

172. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Report and Order, including the Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[427] *See* 5 U.S.C. 801(a)(1)(A).

APPENDIX A

List of Commenters

***Derecho Public Notice* (PS Docket No. 11-60, July 18, 2012)**

Comments:

Arens, Dianna (individual)
Association of Public-Safety Communications Official-International, Inc. (APCO)
AT&T
Biscoe, Gerald (individual)
California Public Utilities Commission (California PUC)
CTIA – The Wireless Association (CTIA)
Duffy, Robert F. (individual)
Fairfax County, Virginia (Fairfax County)
Frontier Communications Corporation (Frontier)
Maryland Public Service Commission
National Association of Broadcasters
National Association of State Utility Consumer Advocates
NENA: The 911 Association (NENA)
Newsom, Les (individual)
Telecommunications Industry Association (TIA)
T-Mobile USA, Inc. (T-Mobile)
Verizon and Verizon Wireless (Verizon)
Virginia State Corporation Commission (Virginia SCC)
Wherry, Phil (individual)

Reply Comments:

AT&T
California PUC
CTIA
Loudoun County, Virginia
MetroPCS Communication, Inc.
Montgomery County, Maryland
National Association of Telecommunications Officers and Advisors (NATOA)
Sindell, Ivan/Global Communications System Research
Standley, Brandon, Chief of Police, Bellefontaine, Ohio
Verizon

Ex Parte Submissions:

Arlington County, Virginia, Information Technology Advisory Commission (Arlington, Co, VA)
Metropolitan Washington Council of Governments (MWCOG)

***911 Reliability NPRM* (PS Docket No. 13-75, March 20, 2013)**

Comments:

Alaska Communications Systems
Alexandria, Virginia
Alliance for Telecommunications Industry Solutions (ATIS)
American Cable Association (ACA)
Arlington County, Virginia
APCO
Assure911.net, LLC
AT&T
Blooston Rural Carriers
Boulder Regional Emergency Telephone Service Authority
California PUC
EchoStar Corporation
Edison Electric Institute
Fairfax County
Falls Church, Virginia
Frontier
Mission Critical Partners, Inc.
NATOA
NENA
NTCA – The Rural Broadband Association (NTCA)
Pennsylvania Public Utility Commission
Secure Commonwealth (Virginia) E911 Sub-Panel
TIA
Texas 911 Alliance
United States Telecom Association (US Telecom)
Utilities Telecom Council
Verizon
Virginia SCC
Western Telecommunications Alliance

Reply Comments:

ACA
AT&T
CenturyLink
Frontier
National Cable & Telecommunications Association (NCTA)
National Tribal Telecommunications Association
NENA
New York City
Verizon

Ex Parte Submissions:

APCO
AT&T
California PUC
CenturyLink
EchoStar Corp. & Hughes Network Systems, LLC
Frontier
Intrado, Inc.
Michael Pope (Electrical Generating Systems Association)
NENA
NTCA
US Telecom
Verizon

APPENDIX B

Final Rules

PART 0 – COMMISSION ORGANIZATION

Section 0.392 is revised to add new subsection (j) to read as follows:

§ 0.392 Authority Delegated.

* * * * *

(j) The Chief of the Public Safety and Homeland Security Bureau is delegated authority to administer the communications reliability and redundancy rules and policies contained in Part 12 of this chapter, develop and revise forms and procedures as may be required for the administration of Part 12, review certifications filed in connection therewith, and order remedial action on a case-by-case basis to ensure the reliability of 911 service in accordance with such rules and policies.

*** * * * ***

Section 0.457 is revised to add new subsection (d)(1)(viii):

§ 0.457 Records not routinely available for public inspection.

* * * (d) *Trade secrets and commercial or financial information obtained from any person and privileged or confidential—categories of materials not routinely available for public inspection, 5 U.S.C. 552(b)(4) and 18 U.S.C. 1905.*

* * * (viii) Information submitted with a 911 reliability certification pursuant to 47 C.F.R. § 12.4 that consists of descriptions and documentation of alternative measures to mitigate the risks of nonconformance with certification elements, information detailing specific corrective actions taken with respect to certification elements, or supplemental information requested by the Commission with respect to such certification.

* * * * *

PART 4 – DISRUPTIONS TO COMMUNICATIONS

Section 4.9 is amended by adding subsection (h) to read as follows:

§ 4.9 Outage reporting requirements – threshold criteria.

* * * * *

(h) *Covered 911 Service Providers*. In addition to any other obligations imposed in this section, within thirty minutes of discovering an outage that potentially affects a 911 special facility (as defined in § 4.5), all Covered 911 Service Providers (as defined in § 12.4(a)(4)) shall notify as soon as possible but no later than thirty minutes after discovering the outage any official who has been designated by the affected 911 special facility as the provider's contact person(s) for communications outages at that facility and convey all available information that may be useful in mitigating the effects of the outage, as well as a name, telephone number, and e-mail address at which the service provider can be reached for follow-up. The Covered 911 Service Provider shall communicate additional material information to the affected 911

special facility as it becomes available, but no later than two hours after the initial contact. This information shall include the nature of the outage, its best-known cause, the geographic scope of the outage, the estimated time for repairs, and any other information that may be useful to the management of the affected facility. All notifications shall be transmitted by telephone and in writing via electronic means in the absence of another method mutually agreed upon in advance by the 911 special facility and the Covered 911 Service Provider.

* * * * *

PART 12 – REDUNDANCY OF COMMUNICATIONS SYSTEMS

The name of Part 12 of 47 C.F.R. is revised to read as follows:

PART 12 – RESILIENCY, REDUNDANCY, AND RELIABILITY OF COMMUNICATIONS

* * * * *

Section 12.4 is added to read as follows:

§ 12.4 Reliability of Covered 911 Service Providers

(a) *Definitions.* Terms in this section shall have the following meanings:

(1) *Aggregation Point.* A point at which network monitoring data for a 911 Service Area is collected and routed to a network operations center (NOC) or other location for monitoring and analyzing network status and performance.

(2) *Certification.* An attestation by a Certifying Official, under penalty of perjury, that a Covered 911 Service Provider:

(i) Has satisfied the obligations of subsection (c) of this section.

(ii) Has adequate internal controls to bring material information regarding network architecture, operations, and maintenance to the Certifying Official's attention.

(iii) Has made the Certifying Official aware of all material information reasonably necessary to complete the certification.

(iv) The term "Certification" shall include both an Annual Reliability Certification under subsection (c) of this section and an Initial Reliability Certification under subsection (d)(1) of this section, to the extent provided under subsection (d)(1).

(3) *Certifying Official.* A corporate officer of a Covered 911 Service Provider with supervisory and budgetary authority over network operations in all relevant service areas.

(4) *Covered 911 Service Provider.*

(i) Any entity that:

(A) Provides 911, E911, or NG911 capabilities such as call routing, automatic location information (ALI), automatic number identification (ANI), or the

functional equivalent of those capabilities, directly to a public safety answering point (PSAP), statewide default answering point, or appropriate local emergency authority as defined in sections 64.3000(b) and 20.3; and/or

(B) Operates one or more central offices that directly serve a PSAP. For purposes of this section, a central office directly serves a PSAP if it hosts a selective router or ALI/ANI database, provides equivalent NG911 capabilities, or is the last service-provider facility through which a 911 trunk or administrative line passes before connecting to a PSAP.

(ii) The term "Covered 911 Service Provider" shall not include any entity that:

(A) Constitutes a PSAP or governmental authority to the extent that it provides 911 capabilities; or

(B) Offers the capability to originate 911 calls where another service provider delivers those calls and associated number or location information to the appropriate PSAP.

(5) *Critical 911 Circuits.* 911 facilities that originate at a selective router or its functional equivalent and terminate in the central office that serves the PSAP(s) to which the selective router or its functional equivalent delivers 911 calls, including all equipment in the serving central office necessary for the delivery of 911 calls to the PSAP(s). Critical 911 Circuits also include ALI and ANI facilities that originate at the ALI or ANI database and terminate in the central office that serves the PSAP(s) to which the ALI or ANI databases deliver 911 caller information, including all equipment in the serving central office necessary for the delivery of such information to the PSAP(s).

(6) *Diversity Audit.* A periodic analysis of the geographic routing of network components to determine whether they are Physically Diverse. Diversity Audits may be performed through manual or automated means, or through a review of paper or electronic records, as long as they reflect whether Critical 911 Circuits are Physically Diverse.

(7) *Monitoring Links.* Facilities that collect and transmit network monitoring data to a NOC or other location for monitoring and analyzing network status and performance.

(8) *Physically Diverse.* Circuits or equivalent data paths are Physically Diverse if they provide more than one physical route between end points with no common points where a single failure at that point would cause both circuits to fail. Circuits that share a common segment such as a fiber-optic cable or circuit board are not Physically Diverse even if they are logically diverse for purposes of transmitting data.

(9) *911 Service Area.* The metropolitan area or geographic region in which a Covered 911 Service Provider operates a Selective Router or the functional equivalent to route 911 calls to the geographically appropriate PSAP.

(10) *Selective Router.* A 911 network component that selects the appropriate destination PSAP for each 911 call based on the location of the caller.

(11) *Tagging.* An inventory management process whereby Critical 911 Circuits are labeled in circuit inventory databases to make it less likely that circuit rearrangements will

compromise diversity. A Covered 911 Service Provider may use any system it wishes to tag circuits so long as it tracks whether Critical 911 Circuits are Physically Diverse and identifies changes that would compromise such diversity.

(b) *Provision of Reliable 911 Service.* All 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. Performance of the elements of the Certification set forth in subsections (c)(1)(i), (c)(2)(i), and (c)(3)(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) *Annual Reliability Certification.* One year after the Initial Reliability Certification described in subsection (d)(1) of this section and every year thereafter, a Certifying Official of every Covered 911 Service Provider shall submit a Certification to the Commission as follows.

(1) *Circuit Auditing.*

(i) A Covered 911 Service Provider shall certify whether it has, within the past year:

(A) Conducted Diversity Audits of Critical 911 Circuits or equivalent data paths to any PSAP served;

(B) Tagged such Critical 911 Circuits to reduce the probability of inadvertent loss of diversity in the period between audits; and

(C) Eliminated all single points of failure in Critical 911 Circuits or equivalent data paths serving each PSAP.

(ii) If a Covered 911 Service Provider does not conform with the elements in subsection (c)(1)(i)(C) above with respect to the 911 service provided to one or more PSAPs, it must certify with respect to each such PSAP:

(A) Whether it has taken alternative measures to mitigate the risk of Critical 911 Circuits that are not Physically Diverse or is taking steps to remediate any issues that it has identified with respect to 911 service to the PSAP, 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.

(2) *Backup Power.*

(i) With respect to any central office it operates that directly serves a PSAP, a Covered

911 Service Provider shall certify whether it:

(C) Provisions backup power through fixed generators, portable generators, batteries, fuel cells, or a combination of these or other such sources to maintain full-service functionality, including network monitoring capabilities, for at least 24 hours at full office load or, if the central office hosts a Selective Router, at least 72 hours at full office load; provided, however, that any such portable generators shall be readily available within the time it takes the batteries to drain, notwithstanding potential demand for such generators elsewhere in the service provider's network.

(D) Tests and maintains all backup power equipment in such central offices in accordance with the manufacturer's specifications;

(E) Designs backup generators in such central offices for fully automatic operation and for ease of manual operation, when required;

(F) Designs, installs, and maintains each generator in any central office that is served by more than one backup generator as a stand-alone unit that does not depend on the operation of another generator for proper functioning.

(ii) If a Covered 911 Service Provider does not conform with all of the elements in subsection (c)(2)(i) above, it must certify with respect to each such central office:

(A) Whether it has taken alternative measures to mitigate the risk of a loss of service in that office due to a loss of power or is taking steps to remediate any issues that it has identified with respect to backup power in that office, 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) *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.

(ii) If a Covered 911 Service Provider does not conform with all of the elements in

subsection (c)(3)(i)(C) above, it must certify with respect to each such 911 Service Area:

(A) Whether it has taken alternative measures to mitigate the risk of network monitoring facilities that are not Physically Diverse or is taking steps to remediate any issues that it has identified with respect to diverse network monitoring in that 911 Service Area, 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.

(d) Other Matters

(1) *Initial Reliability Certification.* One year after the effective date of this rule, a Certifying Official of every Covered 911 Service Provider shall certify to the Commission that it has made substantial progress toward meeting the standards of the Annual Reliability Certification described in subsection (c) of this section. Substantial progress in each element of the certification shall be defined as compliance with standards of the full certification in at least 50 percent of the Covered 911 Service Provider's Critical 911 Circuits, central offices that directly serve PSAPs, and independently monitored 911 Service Areas.

(2) *Confidential Treatment.*

(i) The fact of filing or not filing an Annual Reliability Certification or Initial Reliability Certification and the responses on the face of such certification forms shall not be treated as confidential.

(ii) Information submitted with or in addition to such Certifications shall be presumed confidential to the extent that it consists of descriptions and documentation of alternative measures to mitigate the risks of nonconformance with certification elements, information detailing specific corrective actions taken with respect to certification elements, or supplemental information requested by the Commission or Bureau with respect to a certification.

(3) *Record Retention.* A Covered 911 Service Provider shall retain records supporting the responses in a Certification for two years from the date of such Certification, and shall make such records available to the Commission upon request. To the extent that a Covered 911 Service Provider maintains records in electronic format, records supporting a Certification hereunder shall be maintained and supplied in an electronic format.

(i) With respect to Diversity Audits of Critical 911 Circuits, such records shall include, at a minimum, audit records separately addressing each such circuit, any internal report(s) generated as a result of such audits, records of actions taken pursuant to the audit results, and records regarding any alternative measures taken to mitigate the risk of Critical 911 Circuits that are not Physically Diverse.

(ii) With respect to backup power at central offices, such records shall include, at a

minimum, records regarding the nature and extent of backup power at each central office that directly serves a PSAP, testing and maintenance records for backup power equipment in each such central office, and records regarding any alternative measures taken to mitigate the risk of insufficient backup power.

(iii) With respect to network monitoring, such records shall include, at a minimum, records of Diversity Audits of Monitoring Links, any internal report(s) generated as a result of such audits, records of actions taken pursuant to the audit results, and records regarding any alternative measures taken to mitigate the risk of Aggregation Points and/or Monitoring Links that are not Physically Diverse.

* * * * *

APPENDIX C

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), an Initial Regulatory Flexibility Analysis (IRFA) was incorporated in the *Notice of Proposed Rule Making* (*Notice* or *NPRM*). The Commission sought written public comment on the proposals in the Notice, including comment on the IRFA. The comments received are discussed below. This present Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.

A. Need for, and Objectives of, the Report and Order.

2. In this proceeding, the Commission adopts rules to improve the reliability and resiliency of 911 communications networks nationwide by ensuring that service providers (1) adhere to vital best practices or reasonable alternative measures to mitigate the risk failure and (2) provide public safety answering points (PSAPs) with timely and actionable notification of 911 outages. Specifically, we adopt rules requiring "Covered 911 Service Providers" to take reasonable measures in three key areas to ensure reliable 911 service and submit an annual certification of adherence to essential practices regarding (1) circuit diversity auditing, (2) backup power at central offices that directly serve PSAPs, and (3) diverse network monitoring. To allow flexibility and account for differences in network architecture, service providers may also certify that they have taken reasonable alternative measures to mitigate the risk of 911 service failure, so long as they briefly explain why such measures are reasonable under the circumstances and provide supporting documentation to the Commission upon request. In addition, we amend our outage reporting rules to clarify Covered 911 Service Providers' obligations to provide PSAPs with timely and actionable notification of outages affecting 911 service.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

3. No comments were submitted specifically in response to the IRFA. A broad range of commenters agree with the goal of improving 911 reliability, although some expressed concerns about the anticipated cost of complying with any rules the Commission might adopt.[1] For example, Alaska Communications Systems (ACS), Blooston Rural Carriers, NTCA - The Rural Broadband Association (NTCA), and the Western Telecommunications Alliance (WTA) comment that new regulations promoting best practices could negatively affect small government jurisdictions and small industry. ACS states that "it is not always possible to follow every industry best practice in remote areas such as the Alaska bush."[2] Blooston states that rural carriers already have limited personnel and numerous reporting requirements, and that implementing additional requirements would be overly burdensome.[3] Moreover, Blooston states that "there is no indication in the *Derecho Report* that there are significant failures by rural ILECs," and that any additional reporting requirements should be limited to carriers that experienced failures.[4] WTA states that it "does not believe that there is a clear and established need for expanded new nationwide 911 service requirements and reporting rules for all service providers at this time," and that the proposed requirements and procedures will be "unduly burdensome and expensive for RLECs and other small entities."[5] NTCA states that the Commission should "refrain from implementing new requirements for physical diversity upon small rural carriers" due to their size, limited control over

[1] *See supra*, ¶¶ 73-79 (discussing anticipated incremental cost of rules and addressing service providers' objections).

[2] *See* Alaska Communications Systems Comments at 3.

[3] *See* Blooston Rural Carriers Comments at 2,

[4] *See id.* at 7.

[5] *See* Western Telecommunications Alliance Comments at 1, 3.

interconnecting agreements, and the limited availability of diverse transport routes.[6] NTCA adds that rural carriers should not be subject to additional backup power requirements.[7]

4. The IRFA solicited comment on the impact of the proposed rules to small businesses, as required by the RFA. The Commission sought comment on alternatives for rural carriers including: 1) the establishment of different compliance and reporting requirements; 2) clarification, consolidation, or simplification of compliance or reporting requirements 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. Regarding Blooston's comment in which it objected to burdensome reporting requirements and proposed to limit additional requirements to those carriers which experienced failures in the June 2012 derecho, we conclude that reliability and resiliency of critical 911 communications infrastructure is a nationwide concern that is not limited to the service providers directly affected by the derecho. Rather, the record indicates vulnerabilities that likely exist nationwide and have not been resolved on a purely voluntary basis.[8] In too many cases, the Commission has found that neither voluntary best practices nor other compensating steps (*e.g.* carriers following their own internal practices) were sufficiently implemented to safeguard the public's access to 911 call centers on a nationwide basis.

5. Commenters uniformly agree that industry-led best practices, such as those developed by CSRIC, reflect the best available consensus on appropriate steps to ensure 911 network reliability and resiliency. CSRIC's prioritization of many of these best practices as either "critical" or "highly important" to maintaining reliable communications further suggest that they are cost-effective and likely to achieve their objectives. To the extent that some commenters argue that such best practices may not be applicable in all cases and should therefore be purely voluntary, we note that the certification adopted here allows flexibility for Covered 911 Service Providers to implement specific best practices or reasonable alternative measures in the manner most appropriate for their networks. Regarding NTCA's comment that the Commission refrain from imposing physical diversity requirements and backup power requirements on rural carriers, the rules adopted here allow Covered 911 Service Providers to certify reasonable alternative measures to mitigate the risk of failure where physical diversity and the specified level of backup power may not be feasible. Moreover, the backup power portion of the certification applies only to those central offices that directly serve a PSAP, or approximately one-quarter of all central offices. Service providers may also demonstrate that specific certification elements are not applicable based on their network architecture. Thus, the rules we adopt allow small and rural entities to comply with minimum cost and reporting burden so long as their efforts to provide reliable 911 service are reasonable under the circumstances.

C. Description and Estimate of the Number of Small Entities to Which Rules Will 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 rules adopted herein. The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction." In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act. 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).

7. 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 that

[6] *See* NTCA Comments at 2.

[7] *Id.*

[8] *See supra*, ¶¶ 33-35 (discussing 911 reliability issues beyond the June 2012 derecho).

encompass entities that could be directly affected by the proposals under consideration.[9] As of 2009, small businesses represented 99.9% of the 27.5 million businesses in the United States, according to the SBA.[10] Additionally, 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, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[13] Census Bureau data for 2007 indicate that there were 89,527 governmental jurisdictions in the United States.[14] We estimate that, of this total, as many as 88,761 entities may qualify as "small governmental jurisdictions."[15] Thus, we estimate that most governmental jurisdictions are small.

8. Except for amendments to our existing outage reporting rules, the rules adopted here focus narrowly on entities that provide key facilities for 911 service rather than the broader class of all communications services capable of placing 911 calls. Like the Derecho Report, the Report and Order defines "911 service provider" as a communications provider responsible for routing and delivering 911 calls and location information directly to PSAPs. Under current technologies, these providers are typically ILECs, although the transition to NG911 may broaden the class of entities that provide 911 service in the future.

9. *Small Incumbent Local Exchange Carriers.* We have included small incumbent local exchange carriers in this present RFA analysis. As noted above, a "small business" under the RFA is one that, inter alia, meets the pertinent small business size standard (*e.g.*, a telephone communications business having 1,500 or fewer employees), and "is not dominant in its field of operation." The SBA's Office of Advocacy contends that, for RFA purposes, small incumbent local exchange carriers are not dominant in their field of operation because any such dominance is not "national" in scope. We have therefore included small incumbent local exchange carriers in this RFA analysis, although we emphasize that this RFA action has no effect on Commission analyses and determinations in other, non-RFA contexts.

[9] *See* 5 U.S.C. § 601(3)–(6).

[10] *See* SBA, Office of Advocacy, "Frequently Asked Questions," available at http://web.sba.gov/faqs/faqindex.cfm?areaID=24 (last visited Aug. 31, 2012).

[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).

[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 local 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 52,095. If we make the same population assumption about special districts, specifically that they are likely to have a population of 50,000 or less, and also assume that special districts are different from county, municipal, township, and school districts, in 2007 there were 37,381 such special districts. Therefore, there are a total of 89,476 local government organizations. As a basis of estimating how many of these 89,476 local government organizations were small, in 2011, we note that there were a total of 715 cities and towns (incorporated places and minor civil divisions) with populations over 50,000. CITY AND TOWNS TOTALS: VINTAGE 2011 – U.S. Census Bureau, *available at* http://www.census.gov/popest/data/cities/totals/2011/index.html. If we subtract the 715 cities and towns that meet or exceed the 50,000 population threshold, we conclude that approximately 88,761 are small. U.S. CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES 2011, Tables 427, 426 (Data cited therein are from 2007).

10. *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, and wireless video services.[16] 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.[17] For this category, census data for 2007 show that there were 11,163 establishments that operated for the entire year.[18] Of this total, 10,791 establishments had employment of 999 or fewer employees and 372 had employment of 1000 employees or more.[19] 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 our proposed action.[20]

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

11. In this *Report and Order*, we adopt rules requiring "Covered 911 Service Providers" to take reasonable measures in three key areas to ensure reliable 911 service and submit an annual certification of adherence to essential practices or reasonable alternative measures regarding circuit diversity auditing, backup power at central offices that directly serve PSAPs, and diverse network monitoring. Under these rules, a Covered 911 Service Provider can satisfy its obligation if it performs every element of the certification in each substantive area. Service providers may also certify that they have taken reasonable alternative measures to mitigate the risk of failure or are in the process of remediating vulnerabilities so long as they briefly explain such measures or remediation steps and why they are reasonable and provide supporting documentation to the Commission upon request. Similarly, service providers may respond that a certification element is not applicable to their networks, but they must include a brief explanation of why the element does not apply.

12. If a Covered 911 Service Provider relies on alternative measures in lieu of specific certification elements, the Bureau may conduct a more detailed review to determine whether its measures are nevertheless reasonably adequate to ensure reliable 911 service. Where information revealed through the outage reporting process or available through public sources indicates unresolved vulnerabilities in a service provider's 911 network, the Commission may request additional information, require remedial action to correct those vulnerabilities, or refer the matter to the Enforcement Bureau for further action as appropriate.

13. In addition, we amend our outage reporting rules under Part 4 to clarify Covered 911 Service Providers' obligations to provide PSAPs with timely and actionable notification of outages affecting 911 service. These amendments respond to reports of untimely or inadequate notification during the June 2012 derecho and provide more specific guidance on how 911 call centers can expect to be notified in the event of a 911 service failure.

---

[16] http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517210&search=2007%20NAICS%20Search

[17] 13 C.F.R. § 121.201, NAICS code 517210.

[18] 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).

[19] http://factfinder2.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2007_US_51SSSZ2&prodType=table *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."

[20] *See http://factfinder2.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2007_US_51SSSZ2&prodType=table*

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

14. The RFA requires an agency to describe any significant alternatives that it has considered in developing its 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 and reporting requirements under the rule for such 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 such small entities."

15. Although we sought and received comments on possible exemptions or waivers for small or rural entities, we conclude that overriding public safety concerns require our rules to apply equally to all Covered 911 Service Providers. While we acknowledge that small or rural service providers may have limited resources or operate in remote areas, 911 is no less a critical public service in any part of the nation, and we decline to establish two tiers of 911 reliability based on economics or geography. Accordingly, we intend the certification requirement adopted here to apply to all Covered 911 Service Providers, as defined above,[21] without exceptions based on size or location, and we also decline to create a specific waiver procedure for entities to seek exemption from the rules. We emphasize, however, that the certification approach we adopt allows flexibility for small or rural providers to comply with our rules in the manner most appropriate for their networks, and certain requirements will, by their nature, only apply to larger providers. Moreover, the approaches proposed in the *Report and Order* are intended to complement and strengthen, not to replace, the Commission's current approach of encouraging service providers to voluntarily implement best practices and measuring compliance through outage reporting. Thus, with respect to everyday commercial communications that do not impact public safety as much as 911, small entities with limited resources will 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.

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

16. None.

G. Report to Congress

17. The Commission will send a copy of the Report and Order, including this FRFA, in a report to be sent to Congress pursuant to the Congressional Review Act. In addition, the Commission will send a copy of the Report and Order, including this FRFA, to the Chief Counsel for Advocacy of the SBA. A copy of the Report and Order and FRFA (or summaries thereof) will also be published in the Federal Register.

H. Report to Small Business Administration

18. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Report and Order, including the Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

[21] *See supra*, ¶¶ 36-43 (defining term and discussing nationwide importance of 911 reliability).

STATEMENT OF
CHAIRMAN THOMAS E. WHEELER

Re: *Improving 911 Reliability*, PS Docket No. 13-75; *Reliability and Continuity of Communications Networks, Including Broadband Technologies*, PS Docket No. 11-60.

Since my first day, I've spoken about how the FCC's policies should be guided by what I call the Network Compact – the basic rights of consumers and the basic responsibilities of network operators. This item to improve 911 reliability advances one of the three key elements of the Network Compact – promoting public safety and security.

Today's item is the culmination of a significant amount of work, which began long before I arrived. The derecho storm that ripped through portions of the Midwest and Mid-Atlantic brought widespread 911 network failures across six states and left millions of Americans unable to call for help. The Commission immediately launched an inquiry to examine the major vulnerabilities in 911 network architecture, maintenance, and operations revealed by the storm.

Regrettably, many of the 911 outages could have been avoided if the wireline 911 service providers had implemented best practices – in fact, best practices that the industry had helped to develop – and other sound engineering principles.

I have spoken of the "regulatory see-saw." When the marketplace works, the reasons for regulation are diminished. Part and parcel with that belief, I also have said that the Commission should encourage multi-stakeholder solutions to network responsibilities.

Inherent in the regulatory see-saw is the reality that if voluntary solutions don't work, we must be willing to pivot rapidly to a regulatory response. This is especially true when public safety is at stake.

The 2012 derecho demonstrated how the industry failed to take the proper steps to prevent these kinds of widespread outages. As such, we have an obligation and responsibility to act.

The result of the hard work put forth by the Bureau and my colleagues and predecessors is the necessary, sensible, and flexible set of rules we are adopting today, which will help assure that Americans can reach emergency assistance during disasters.

Our rules are flexible – they account for differences in 911 network architecture – but we do not sacrifice 911 service reliability. Consistent with the old axiom, 'if you can't measure it, you can't manage it," we are putting such measurement and management tools in place. We require 911 service providers to take reasonable measures to provide reliable 911 service and to certify annually that they have done so. They can either follow certain industry-backed best practices or implement alternative measures that are reasonable and sufficient to achieve the necessary result in light of their particular circumstances. Our rules also provide greater clarity on how these critical industry-backed best practices should be implemented in the context of 911 networks.

Moreover, to accommodate evolving technology, these rules take into account the transition to Next Generation 911. To keep up with technology, we will re-evaluate the rules in five years.

In addition, today's Order will help ensure that 911 call centers get timely and useful information about 911 outages.

I recognize that 911 service providers may have made improvements since the derecho. But given the 911 failures of the past, and with public safety at stake, the Commission cannot simply trust - we must also verify. Or, as a wise man once taught me, “inspect what you expect.”

I am pleased to support this Order and thank the staff of the Public Safety and Homeland Bureau for their work on this important item.

STATEMENT OF
COMMISSIONER MIGNON L. CLYBURN

Re: *Improving 911 Reliability*, PS Docket No. 13-75; *Reliability and Continuity of Communications Networks, Including Broadband Technologies*, PS Docket No. 11-60.

Congress made public safety a fundamental purpose for creating this agency almost 80 years ago. It also passed laws, in 1999 and 2008, that authorize us to promote emergency 9-1-1 services throughout the country. So, whenever the FCC identifies significant problems with these vital services, we should not hesitate to address them, and by adopting this Order, the Commission takes necessary action to improve the reliability of emergency networks.

The 9-1-1 problems which this Order addresses came to our attention at a time when we could least afford them -- during the June 2012 derecho -- one of the most disastrous storms our Nation has experienced. Even though it lasted less than a day, the storm resulted in 22 deaths, widespread damage, and millions of power outages across several Midwest and Mid-Atlantic states. The derecho also impaired the ability of millions of Americans to access 9-1-1 services and left certain areas without 9-1-1 for several days.

The Commission thoroughly investigated and reported on why these service outages occurred. The staff reviewed more than 500 network outage reports, and interviewed 28 PSAPs and representatives from eight communications providers. What the staff found was that with regard to a number of service providers, 9-1-1 service disruptions were due to companies failing to have adequate plans and systems in place during storms, and other inclement weather events. In other words, these failures could have been avoided if these providers had followed industry best practices developed by CSRIC – our advisory committee on network security and reliability.

Because addressing these concerns should be a high priority, I circulated a draft Order to improve the reliability of these networks with four core requirements that our staff recommended in its report. 9-1-1 service providers must: audit the physical routes of their networks; ensure physical diversity of monitoring links; require a specific amount of backup power at central offices; and give PSAPs more information when and where service outages occur.

I wish to thank Chairman Wheeler for placing this Order on the agenda for today's Open Meeting and I am grateful to Lisa Fowlkes, Jeff Goldthorp, Eric Schmidt, and the other talented staff members who contributed to this excellent Order. I join others in welcoming Admiral David Simpson to the Commission, congratulate him on his appointment as Chief of the Public Safety and Homeland Security Bureau, and thank David Turetsky for his contributions to the item.

STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL

Re: *Improving 911 Reliability*, PS Docket No. 13-75; *Reliability and Continuity of Communications Networks, Including Broadband Technologies*, PS Docket No. 11-60.

During the Summer before last, a fast-moving storm known as a Derecho blew through the Midwest and Mid-Atlantic. These were not the usual warm winds of late June. These were gusts of up to 80 miles per hour. And they were accompanied by sheets of rain and bolts of lightning.

The damage left in the wake of the Derecho was substantial. This was Mother Nature at her most angry. We had downed trees, blocked roads, power outages—and serious failures in our communications systems.

To learn more, in the days following the Derecho I visited the 911 center in Fairfax County, Virginia. The head of Fairfax County's Department of Public Safety Communications described an eerie quiet in the aftermath of the storm, as calls into 911 quickly and implausibly ceased. He said he knew instantly something was wrong. He was right.

In fact, during the Derecho, 77 public safety answering points spanning six states lost some connectivity. This affected more than 3.6 million people. Seventeen 911 call centers lost service completely. This left more than two million people without access to 911 during and after the storm. It was many hours before the calls returned—and in some cases days. This is unacceptable. It puts the safety of too many people at risk.

So it was clear that we needed an investigation. Because when things like this happen we have to search out the facts—wherever they lead. Then we need to apply the lessons we learn. Not just in the Midwest and Mid-Atlantic where the Derecho struck—but everywhere.

The staff at the Commission has done extraordinary work to understand what happened. They worked with carriers, reached out to public safety officials, and combed through lots and lots of paper. As a result, we now know that as many as nine generators failed to start, disabling hundreds of network transportation systems. We know that back-up generators and switches failed. We also know that power failures undermined network monitoring capabilities.

So we understand what did not go right. Now we are doing something about it. The rules we adopt today require 911 service providers to adopt practices for auditing circuit diversity, to supply back-up power to central offices that service 911 call centers, and to provide diverse network monitoring. We also direct providers to reach out to 911 call centers and let them know when they experience a service outage, so first responders are not left in the dark unable to do their job and help us when the unthinkable occurs.

These are simple, commonsense solutions. But they matter. Because this is not just a conversation about technical fixes. This is a conversation about real people and their safety.

I am grateful to the Chairman for making this a priority so early in his tenure. Thank you also the Public Safety and Homeland Security Bureau for your continued diligence. Your efforts have my full support.

DISSENTING STATEMENT OF COMMISSIONER AJIT PAI

Re: *Improving 911 Reliability*, PS Docket No. 13-75; *Reliability and Continuity of Communications Networks, Including Broadband Technologies*, PS Docket No. 11-60.

When our citizens call 911, they expect and deserve to reach emergency personnel. Making that happen for each and every 911 call is not easy. Unlike normal calls, a consumer's provider—whether a traditional telephone carrier or a wireless operator, a cable company or an over-the-top, interconnected VoIP provider—cannot simply transmit a 911 call to a destination based on the number dialed. Instead, that provider must transmit the call to a selective router to determine which public safety answering point (PSAP) should receive the call. Then it must determine how to connect that caller to that PSAP. The PSAP in turn queries an automatic location information (ALI) database to determine the location of the caller so that emergency personnel can respond immediately. PSAPs themselves purchase communications services from 911 system service providers (SSPs), all under the oversight of state governments.

Notably absent from this arrangement is the FCC. We do not establish 911 service tariffs. We do not negotiate 911 service contracts. And we do not collect or distribute 911 funds. Instead, Congress has given us a supplementary role when it comes to 911 SSPs: We are charged with "work[ing] cooperatively with public safety organizations [and] industry participants . . . to develop best practices" for "network diversity requirements," "call-handling in the event of call overflow or network outages," and "certification and testing requirements" for service to PSAPs.[1]

For years, the Commission has carried out this statutory duty through its Communications Security, Reliability, and Interoperability Council (CSRIC), and its predecessors. CSRIC has developed and maintained best practices for network reliability and disaster preparedness. Most 911 SSPs have claimed that they voluntarily follow these best practices. Unsurprisingly, many PSAPs have relied on these promises in evaluating the service of 911 SSPs.

The 2012 derecho storm that swept across the Mid-Atlantic states revealed a flaw in this voluntary scheme. Although some 911 SSPs claimed to follow best practices, their performance during and after the derecho confirmed that they did not do so consistently. And because these providers' claims of compliance were never formally made to the Commission, we had little authority to take action against those who had broken their promises.

Given this background, the Commission needed to take steps within its power to correct the situation. For example, we could have required 911 SSPs to formally certify whether or not they comply with industry best practices. This would let PSAPs know which providers do not conform to best practices and enable PSAPs to order corrective action. This would also make providers' promises enforceable and enable the Commission to sanction those filing false certifications. As a second step, we could have required an across-the-board audit of critical 911 circuits so that all 911 SSPs—and, crucially, their customers, the PSAPs—could identify weaknesses in today's 911 service infrastructure. Indeed, I would have supported today's item had we taken just these steps, and I proposed to align this order with that vision.

[1] Wireless Communications and Public Safety Act of 1999, Pub. L. 106-81, § 6(h), *as amended by* New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. No. 110-283, § 101(2).

But today's order goes a hop, skip, and a long jump further. For example, while the *Order* claims to adopt a certification scheme, it in fact adopts extremely prescriptive and mandatory standards. Take new rule 12.4(b). This rule requires 911 SSPs to "take reasonable measures to provide reliable 911 service." This sounds anodyne in theory. But in practice, it gives the Commission carte blanche to fine 911 SSPs that do not comply with whatever particular practices the Commission demands.[2] As such, a 911 SSP must comply with new federal rules, such as annual diversity audits. It must do so even if that information reveals nothing new to the providers or their PSAP customers. And it must do so even though across-the-board annual audits do not come cheap; they are likely to cost the industry anywhere from $8.96 million to $22.4 million each year.[3]

Another problem is that the *Order* claims to leave network design decisions to PSAPs and 911 SSPs but instead delegates freewheeling authority to the Public Safety and Homeland Security Bureau to "order remedial action on a case-by-case basis to ensure the reliability of 911 service."[4] In other words, the Bureau now has the largely unconstrained authority to order a carrier to redesign its network, to purchase new equipment, or to deploy new facilities, if someone in Washington says so. This level of micromanagement, even if the Commission were equipped to carry it out, is neither appropriate nor effective. We at the Commission have not trenched fiber, have not tested back-up power facilities, and have not designed network monitoring facilities. The experience reviewing the performance of 911 networks after a single storm that affected barely one percent of the country's PSAPs does not qualify us to second-guess the negotiated agreements of thousands of PSAPs and their 911 SSPs nationwide.

A third and final problem with the *Order* is that it imposes burdensome regulations that stray far beyond CSRIC best practices. For example, best practices require only "periodic[]" diversity audits "when called for by network design"[5] and advise providers, "where appropriate, to design networks . . . to minimize the impact of a single point of failure."[6] Industry is implementing these practices with audits every two or three years,[7] in part because other best practices, such as circuit tagging, help prevent the need for more frequent audits.[8] Against this backdrop, the NPRM in this proceeding stated that circuit audits should occur every two years and were only "necessary for roughly half of these PSAPs because that is the portion likely to be served by more than one selective router."[9] But what does the *Order* require? Annual audits of *every 911 circuit in the country*.

This will obviously burden 911 SSPs. But ultimately, our nation's PSAPs (and hence taxpayers) will bear these costs. For 911 SSPs, like most other businesses, generally pass on such costs to their customers. Shouldering these additional costs may make some PSAPs think twice before investing in innovative approaches to reliability, such as adopting Next-Generation 911. And ironically, it is not the PSAPs that serve large suburban areas that are most likely to suffer these costs, but those who serve rural areas and tribal lands, flood-prone bayous, soaring mountain communities, and the remote Alaska bush. Those PSAPs must confront how to allocate scarce resources every day. If a Commission-ordered

[2] *See, e.g.*, *Order* at para. 63.

[3] Audits are expected to take 16–40 man-hours, *see Order* at notes 244, 255, at a cost of $80 per hour for each of 7,000 PSAPs.

[4] Rule 0.392(j).

[5] CSRIC Best Practice 8-7-0532.

[6] CSRIC Best Practice 8-7-0402.

[7] *See, e.g.*, Frontier Comments at 9; Verizon *Ex Parte* Notice at 1 (July 3, 2013); CenturyLink *Ex Parte* Notice at 1 (Sept. 18, 2013).

[8] *See, e.g.*, Fairfax County Comments at 4; Frontier Comments at 9.

[9] NPRM at para. 41.

network redesign costs so much that a PSAP must reduce the number of operators it employs—the consequences could be dire.

I understand the urge to take action. Some 911 SSPs did not live up to their commitments in the derecho, and accountability is necessary. But the people these providers failed are their customers, the PSAPs, and those Americans who could not reach emergency services in a time of need, not us in federal government. And it is the PSAPs, the states and municipalities that oversee them, and on-the-ground first responders, not those working in this building, who must be empowered to take the lead. I respectfully dissent.

DISSENTING STATEMENT OF
COMMISSIONER MICHAEL O'RIELLY

Re: *Improving 911 Reliability*, PS Docket No. 13-75; *Reliability and Continuity of Communications Networks, Including Broadband Technologies*, PS Docket No. 11-60.

I have been sincere in my comments that I want to find common ground with my colleagues so items can be approved unanimously. We have an obligation to try to work together for the greater good. Sadly, this is one of those instances where the gap was too wide to bridge. It didn't have to be this way.

The safety of our nation's citizens is not a partisan issue. I take a backseat to no one in trying to ensure Americans are protected in times of need. In fact, everyone supports a fully functioning and reliable 9-1-1 system, especially during major catastrophes. When people's lives are at stake – real life and death matters – our communications networks need to be ready and able to meet the challenges.

The question becomes what is the best way to make sure this happens. I proposed several edits and supported changes proposed by Commissioner Pai that would have narrowed the rules while still meeting that goal. While I appreciate that some small changes were made, the key suggestions of both of us were rejected.

One of my requests was to minimize the burdens on so-called good actors. Let's be clear: I am a strong proponent of strenuously enforcing the Commission's rules. However, we should try to find a way to lessen the burdens over time on the good actors – communications companies whose networks and services are continually operational and meet the Commission's requirements. In other words, do they have a clean checklist and are their alternative measures, if necessary, ensuring reliable 9-1-1 service year after year? This seems immensely reasonable in light of the requirement that certifications be filed annually, instead of biennially, as was the case in the original draft. After a couple certifications, we ought to know those companies that go the extra mile for compliance and probably don't need to be scrutinized under the item's rubric of a never-ending, yearly certification scheme. My idea of a simple waiver process to ease the burdens for good actors was rejected without much debate.

My support for a waiver process is not because I support the free-market and less regulation, which I do. It is because I know that the compliance costs are going to be passed on to consumers – including the struggling families deciding whether to keep phone service – that are going to pay more each month for unnecessary regulations. The Commission has found a way to drive up consumer costs by burdening truly good actors for no real benefit.

I am equally troubled that my simple proposal to replace the vague, non-committal review of the newly imposed rules in five years – a review that is not mandated to be completed – was also dismissed. For too many years and in too many situations, the Commission enacted rules with no mechanism to fully and faithfully determine, in the future, whether such rules should be retained or modified. Accordingly, I proposed a variety of sunsetting mechanisms to ensure that the Commission would have to revisit these 9-1-1 reliability rules in order to preserve them. I even went so far as to propose that the Commission or the Bureau could extend the rules if the certifications and other relevant data showed that there was still a need for the rules. As incredible as it may seem, this was rejected due to a view that the providers should have the burden to request a rulemaking to show that rules should be eliminated. I disagree. What became clear through this process is that there is great resistance to sunsetting Commission rules. For those that want to explore real FCC process reform, let's start there.

For these reasons, I dissent to this Order. Sadly, this was a missed opportunity. It was well within our grasp to produce a 5-0 vote. Despite my dissatisfaction, I thank the staff for all of their hard work. It's on to the next item for me.