6712-01

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 0, 4, and 12

[PS Docket No. 13-75; PS Docket No. 11-60; FCC 13-158]

Improving 9-1-1 Reliability; Reliability and Continuity of Communications Networks, Including Broadband Technologies

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In this document, 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. Providers subject to the rule can comply with the reasonable measures requirement by either implementing certain industry-backed "best practices" the Commission adopted, or by implementing alternative measures that are reasonably sufficient to ensure reliable 911 service. The FCC also requires 911 service providers to provide public safety answering points (PSAPs) with timely and actionable notification of 911 outages.

DATES: Effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** except for §12.4(c) and (d)(1), which contain information collection requirements that have not been approved by Office of Management and Budget. The Federal Communications Commission will publish a document in the Federal Register announcing the effective date.

FOR FURTHER INFORMATION CONTACT: Eric P. Schmidt, Attorney Advisor, Public Safety and Homeland Security Bureau, (202) 418-1214 or eric.schmidt@fcc.gov. For additional

information concerning the Paperwork Reduction Act information collection requirements contained in this document, contact Benish Shah, (202) 418-7866, or send an email to PRA@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Report and Order in PS Docket No. 13-75 and PS Docket No. 11-60, FCC 13-158, released on December 12, 2013. The full text of this document is available for public inspection during regular business hours in the FCC Reference Center, Room CY–A257, 445 12th Street SW., Washington, DC 20554, or online at http://www.fcc.gov/document/fcc-adopts-rules-improve-911-reliability.

I. INTRODUCTION

1. The Commission was spurred to adopt these rules following the devastating impact many telecommunications networks experienced as a result of the unanticipated "derecho" storm in June 2012. 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 FCC's 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. The Commission requires 911 service providers to take "reasonable measures" to provide reliable 911 service, based on best practices developed by the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) advisory committee, with

refinements designed to add clarity and specific guidance regarding how those practices should be implemented in the context of 911 networks. Providers will demonstrate their compliance by filing an annual certification. The certification elements the Commission are based on best practices identified by CSRIC as critical or highly important, indicating that they significantly reduce the potential for a catastrophic failure of communications or – at a minimum – improve the likelihood of emergency call completion.

3. The Commission seeks to maximize flexibility and account for differences in network architectures without sacrificing 911 service reliability. Accordingly, service providers that certify annually that they have implemented certain industry-backed "best practices," will be deemed to satisfy the reasonable measures requirement. Providers may also certify 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. Based on the information included in the certifications, the Commission may require remedial action to correct vulnerabilities in a service provider's 911 network if it determines 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. The Commission delegates authority to the Bureau to review certification information and follow up with service providers as appropriate to address deficiencies revealed by the certification process.

5. The FCC also amends its 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.

II. BACKGROUND

A. 911 Network Architecture

6. The primary function of the 911 network is to route emergency calls to the geographically appropriate PSAP based on the caller's location. 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. 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.

7. Once a 911 call reaches the appropriate PSAP, the PSAP queries an automatic location information (ALI) database to determine the location of the caller. For wireline calls, ALI is based on the address associated with the caller's phone number. For wireless calls, providers use various technologies to determine the caller's location. 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.

8. 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.

NG911 networks offers 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.

B. FCC Approach to Communications Reliability

9. 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. 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. 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.

10. The Commission's mandatory Network Outage Reporting System (NORS) and voluntary Disaster Information Reporting System (DIRS) provide outage data that help gauge whether 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. The Bureau also works with service providers on an

informal basis to identify and resolve communications reliability issues revealed through the outage reporting process.

C. June 2012 Derecho

11. 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 widespread property damage, and left millions of residents without electrical power for as long as two weeks. 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. In contrast, the derecho moved rapidly across multiple states with very little warning, putting critical infrastructure to an unexpected test and revealing significant vulnerabilities in service providers' networks and operations.

12. The derecho's 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. Fairfax County, Virginia noted that the disruption of 911 service 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.

D. PSHSB Derecho Report

13. 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. These interactions clarified and expanded the information the Commission had already received via NORS and DIRS.

14. In its January 2013 Derecho Report, available at http://www.fcc.gov/document/derecho-report-and-recommendations, 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). 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.

E. 911 Reliability Notice of Proposed Rulemaking

15. On March 20, 2013, the Commission adopted a Notice of Proposed Rulemaking (911 Reliability NPRM or NPRM), available at http://www.fcc.gov/document/improving-9-1-1-reliability, which outlined options to implement recommendations from the Derecho Report. These options ranged from reporting and certification obligations, to mandatory reliability requirements supported by site inspections and compliance reviews. The NPRM also proposed to amend the Commission's rules to require 911 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.

III. DISCUSSION

A. Need for Commission Action

16. A primary responsibility of the Commission 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. Consistent with that overarching obligation, the Commission has specific statutory responsibilities with respect to 911 service. The outage reporting process has often been effective in improving the reliability and resiliency of many communications services, and the Commission continues 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. In light of this experience and substantial evidence in the record of this proceeding, the Commission concludes that additional Commission action is both warranted and needed with

respect to critical 911 communications.

B. Entities Subject to the Rules

17. The rules adopted 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 (as that term is defined elsewhere in the Commission's rules), or that operates one or more central offices that directly serve a PSAP. 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.

18. This definition 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, 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. The Commission takes this step in recognition 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, the Commission describes 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.

19. While the FCC strongly supports the transition to NG911, it is 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. The Commission might, however, revisit this distinction in the future as technology evolves, as discussed below with regard to review and sunset of the rules. In a similar vein, the FCC does not adopt a definition that covers all operators of emergency services Internet protocol networks (ESInets). 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, ESInet operators will be required to certify reliability only to the extent they qualify as Covered 911 Service Providers under our rules.

C. Implementation Approach

20. The FCC adopts rules requiring Covered 911 Service Providers to: (1) take reasonable measures to ensure reliable 911 service, and (2) certify annually whether they do so by adhering either to specified practices based on established industry consensus or to alternative measures demonstrated to be reasonably sufficient to mitigate the risk of failure. Regarding reasonable measures, the record in this proceeding demonstrates a number of concrete and objective indications of whether a service provider's practices with respect to 911 reliability are reasonable. For example, best practices are developed in a "consensus-based

environment" reflecting the collective judgment of industry, 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, there should be a reasonable basis for such decisions, coupled with appropriate steps to compensate for any increased risk of failure.

21. Regarding annual certification, a Covered 911 Service Provider that performs and certifies all the specific certification elements outlined in the rules regarding 911 circuit auditing, backup power at central offices that directly serve PSAPs, and diverse network monitoring links, is not required to provide additional documentation to support its certification that it has met the reasonable measures requirement. These providers will be deemed to satisfy the obligation to take reasonable measures to provide reliable 911 service, provided that the certification is accurate and complete. 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. 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. 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.

22. In addition, the Commission will 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. 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, the Commission reserves 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.

23. While the FCC adopts the certification approach, it notes 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. It therefore will require all Covered 911 Service Providers to certify annually to certain basic measures in the three substantive areas, and delegates to the Bureau the responsibility to review the certifications and take additional action as appropriate, and the authority and responsibility to develop the certification form and filing system. The reliability certifications will be subject to penalties for false or misleading statements both under the United States Code and the Commission's rules. The certification shall also be accompanied by a statement explaining the basis for such certification and shall be subscribed to as true under penalty of perjury in substantially the form set forth in section 1.16 of the Commission's rules.

24. Certification Standards. In response to call by some commenters to convene a new group to develop new certification standards and procedures unique to these rules, the Commission notes that the process these commenters describe is virtually indistinguishable from the Commission's existing CSRIC process. These revised CSRIC best practices are available to stakeholders for application on a voluntary basis; the Commission therefore sees no reason to defer its refinement and implementation of these best practices in a Commission rule, in light of its experiences with voluntary standards.

25. The FCC understands that, as NG911 deployment advances, the certification standards may have to change, and the Commission may then need to turn to multi-stakeholder bodies like CSRIC for recommendations in these areas. Accordingly, the Commission adopts certification standards that are consistent with current best practices but also flexible enough to account for differences in 911 and NG911 networks.

26. 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.

27. Effect of Certification. Under the certification process, a Covered 911 Service Provider that performs all the certification elements in a substantive area will be deemed to comply with the requirement to take reasonable measures in that area. This result is subject only to any determination the Commission or as delegated, the Bureau, may make afterward, based on complaints, outage reports or other information, that the Covered 911 Service Provider did not, in fact, perform as claimed in its certification. 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.

28. 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. 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. In extreme cases, such as where a provider is not acting in good faith, the Bureau may also refer cases 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.

29. Certification Phase-In. The rules, including the underlying obligation to take reasonable measures to provide reliable 911 service, become effective thirty days after publication in this 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 Paperwork Reduction Act, 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.

30. 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, the FCC requires 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, "substantial progress" in this context meaning at least 50-percent compliance with each of the three substantive certification requirements. For example, regarding circuit diversity, Covered 911 Service Providers must certify they have conducted at least 50 percent of the circuit audits. The Bureau has delegated authority to implement this initial certification, including the form and process through which it is submitted. 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.

31. Regarding costs and benefits of the Commission's actions, the FCC notes that no

commenter questioned the basic premise that 911 communications provide significant public health and safety benefits, nor provided an alternative method of quantifying the public safety benefits associated with reliable 911 service. Further, the FCC considers it fortunate that the effects of the derecho were not worse given the serious problems it revealed.

32. The 911 Reliability NPRM estimated total costs to service providers of $16.1 million to $44.1 million. By relaxing or eliminating several of the requirements proposed in the NPRM, however, the Commission reduced the impact on service providers far below those estimates. The expected costs also are 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. The FCC finds that its 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 adopted is based on best practices developed through broad industry consensus.

D. Certification requirements

a. Circuit diversity.

33. 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, 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.

34. 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.

35. Covered 911 Service Providers must also retain records of circuit audits for confidential review by the Commission, upon request, for two years.

36. "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 appear in the network (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. Critical 911 circuits also include links from ANI/ALI databases to central offices that serve PSAPs. The definition does not include 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, the auditing obligation extends to data transport paths for the core 911 capabilities, regardless of whether they are technically "circuits." 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."

37. 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. 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, the Commission focuses on physical diversity as the optimum standard for certification, but also recognizes 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. Thus, there is no 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.

38. Auditing method. To be in conformance with CSRIC best practices, 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.

39. Frequency of audits. The FCC concludes 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. Regular auditing of critical 911 circuits can significantly improve network reliability, and the FCC concludes that annual auditing of 911 circuits and network monitoring links is necessary to prevent a loss of diversity in these critical circuits due to routine circuit rearrangements between audits.

40. Corrective measures. 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. The Commission will also require Covered 911 Service Providers to explain why measures short of physical diversity are reasonably sufficient to ensure reliable 911 service in individual cases.

41. Cost effectiveness. 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. The Commission believes that most of these costs associated with these audits 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, it is more likely that only a segment of critical 911 circuits are not already subject to regular audits, 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.

42. All told, commenters provided estimates ranging from $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 and from Frontier and CenturyLink indicating that even their existing auditing methods require less than 40 hours per PSAP, the Commission does not accept that Verizon's considerably-higher estimate accurately represents the cost of our rules to the industry as a whole. Furthermore, the certification's two-year phase-in will allow all Covered 911 Service Providers to reexamine their existing circuit auditing practices and implement more efficient systems. As such, the FCC believes 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. 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. 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.

b. Central office backup power.

43. Covered 911 Service Providers must 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. In addition especially critical central offices that host selective routers must 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.

44. 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 service-provider facility through which a 911 trunk or administrative line passes before connecting to a PSAP. Service providers must also certify whether: (1) 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; (2) adhere to CSRIC best practices regarding fully automatic, non-interdependent generators that can be started manually if necessary; and (3) 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.

45. Because different central offices present different backup power challenges and a single solution may not be suitable for all, Covered 911 Service Providers may 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 allows 911 service providers flexibility to maintain adequate central-office backup power based on best practices and reasonable alternatives to suit site-specific circumstances.

46. Testing standards. The rules require Covered 911 Service Providers, consistent with CSRIC best practice, to certify that they test their backup power equipment according to the relevant manufacturers' specifications. Further, because failure of interdependent generators was a significant factor in the communications failures during the June 2012, the Commission believes that tandem generators should be electronically separated to ensure that failure of one generator does not cause the other to fail, and will require the certification to confirm whether the 911 provider employs stand-alone backup power sources. 911 providers will have the opportunity to demonstrate that alternative measures upon which they rely (e.g., load shedding) are reasonably sufficient to mitigate the risk of failure.

47. Cost effectiveness. The NPRM estimated that the incremental cost incurred to perform backup power certifications, including remediation, ranged from $11.7 million to $37.5 million depending on whether the Commission would require fixed generators at all central offices. The Report and Order includes no such requirement, meaning that there would be no incremental costs for central offices appropriately provisioned with portable generators. As a result, the Commission estimates the cost to conform to its backup power standards is much closer to $11.7 million than $37.5 million. Further, the approach adopted will also significantly reduce the cost of compliance by covering only central offices directly serving PSAPs or hosting selective routers or ALI databases, 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.

c. Network Monitoring

48. Covered 911 Service Providers must 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 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.

49. 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.

50. 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.

51. 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, the Commission believes 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. As such, the 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.

51A. Cost effectiveness. The Commission calculates the costs of network monitoring to be $732,000, as opposed to the $2,196,000 suggested in the NPRM. In the absence of more detailed cost estimates from commenters, the Commission finds that the certification approach 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

52. Covered 911 Service Providers must notify PSAPs of outages potentially affecting 911 service to that PSAP within 30 minutes of discovering the outage and provide contact information such as a name, telephone number, and e-mail for follow-up. 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 the estimated time for repairs.

F. Legal Authority

53. In light of the Commission's 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. A full statement of the Commission's legal authority to adopt these rules is contained in the Report and Order.

G. Confidentiality

54. The Commission recognizes 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, there is 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, 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 will not in and of itself be considered confidential.

55. Nevertheless, 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, certain information will be treated 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. The Commission would expect, without requiring it, 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.

H. Review and Sunset of Rules

56. 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. 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 its 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, it will establish an appropriate sunset date for those portions of the rules that are no longer necessary. The Commission declines 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.

I. Authority Delegated to the Public Safety and Homeland Security Bureau

57. PSHSB has delegated authority to implement the rules adopted in the Report and Order, consistent with the Administrative Procedure Act and relevant portions of the Communications Act. The Commission directs the Bureau to develop such forms and procedures as may be required to collect and process certifications, and 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. The Bureau also has delegated authority 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. Accessible Formats

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

B. Paperwork Reduction Act Analysis

59. The Report and Order 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 interested parties are invited to comment on the new information collection requirements contained in this proceeding.

60. We note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. 3506(c)(4), the Commission previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees. We have described impacts that might affect small businesses, which includes most businesses with fewer than 25 employees, in the FRFA in Appendix C of the Report and Order, paragraphs 14-15.

C. Congressional Review Act

61. The Commission will send a copy of the Report and Order in a report to be sent to

Congress and the Government Accountability Office pursuant to the Congressional Review Act, see 5 U.S.C. 801(a)(1)(A).

D. Final Regulatory Flexibility Analysis

62. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), an Initial Regulatory Flexibility Analysis (IRFA) was included in the NPRM in PS Docket No. 11-60 and PS Docket No. 13-75. The Commission sought written comment on the proposals in this docket, including comment on the IRFA. This Final Regulatory Flexibility Analysis conforms to the RFA.

V. ORDERING CLAUSES

63. 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.

64. IT IS FURTHER ORDERED that parts 0, 4, and 12 of the Commission's rules, 47 CFR Parts 0, 4, and 12, ARE AMENDED, effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** except for §12.4(c) and (d)(1), which contain information collection requirements that have not been approved by Office of Management and Budget. The Federal Communications Commission will publish a document in the Federal Register announcing the effective date.

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

66. 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.

67. 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.

List of Subjects

47 CFR Part 0

Commission organization; Confidential material; Delegation of authority.

47 CFR Part 4

Telecommunications.

47 CFR Part 12

Certification; Telecommunications.

FEDERAL COMMUNICATIONS COMMISSION

Sheryl D. Todd,
Deputy Secretary.

Final Rules

For the reasons set forth in the preamble, the Federal Communications Commission amends 47 CFR parts 0, 4, and 12 as follows:

PART 0 – COMMISSION ORGANIZATION

1. The authority citation for part 0 continues to read as follows:

Authority: Sec. 5, 48 Stat. 1068, as amended; 47 U.S.C. 155.

2. Section 0.392 is revised by adding paragraph (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 of this chapter, 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.

3. Section 0.457 is amended by revising paragraph (d)(1)(viii) to read as follows:

§ 0.457 Records not routinely available for public inspection.

* * * *

(d)* * *

(1)* * *

(viii) Information submitted with a 911 reliability certification pursuant to 47 CFR 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

4. The authority citation for part 4 continues to read as follows:

Authority: Sec. 5, 48 Stat. 1068, as amended; 47 U.S.C. 154, 155, 201, 251, 307, 316, 615a-1, 1302(a), and 1302(b).

5. Section 4.9 is amended by adding paragraph (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) of this chapter) 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 – RESILIENCY, REDUNDANCY AND RELIABILITY OF COMMUNICATIONS

6. The authority citation for part 12 continues to read as follows:

Authority: Sections 1, 4(i), 4(j), 4(o), 5(c), 218, 219, 301, 303(g), 303(j), 303(r), 332, 403, 621(b)(3), and 621(d) of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154(i), 154(j), 154(o), 155(c), 218, 219, 301, 303(g), 303(j), 303(r), 332, 403, 621(b)(3), and 621(d), unless otherwise noted.

7. Revise the heading of part 12 to read as set forth above.

8. 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 paragraph (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 paragraph (c) of this section and an initial reliability certification under paragraph (d)(1) of this section, to the extent provided under paragraph (d)(1) of this section.

(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 §§ 64.3000(b) and 20.3 of this chapter; 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 paragraphs (c)(1)(i), (c)(2)(i), and (c)(3)(i) of this section shall be deemed to satisfy the requirements of this paragraph. 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 paragraph based upon a showing in accordance with paragraph (c) of this section 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 paragraph (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 paragraph (c)(1)(i)(C) of this section 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 paragraph 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:

(A) 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.

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

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

(D) 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

paragraph (c)(2)(i) of this section, 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 paragraph 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

paragraph (c)(3)(i)(C) of this section, 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 paragraph 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 **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, 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 paragraph (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.

[FR Doc. 2014-00958 Filed 01/16/2014 at 8:45 am; Publication Date: 01/17/2014]