cable systems, and DBS providers shall comply with the aural and visual message requirements in §11.51. Special EAS tests at the State and Local Area levels may be conducted on daily basis following procedures in State and Local Area EAS plans.

(b) Entries shall be made in EAS Participant records, as specified in §11.35(a) and 11.54(a)(3).

[70 FR 71038, Nov. 25, 2005, as amended at 76 FR 12604, Mar. 8, 2011; 77 FR 16707, Mar. 22, 2012; 80 FR 37177, June 30, 2015]

PART 12—RESILIENCY, REDUNDANCY AND RELIABILITY OF COMMUNICATIONS

Sec.
12.1 Purpose.
12.3 911 and E911 analyses and reports.
12.4 Reliability of covered 911 service providers.
12.5 Backup power obligations.

AUTHORITY: Sections 1, 4(i), 4(j), 4(o), 5(c), 201(b), 214(d), 218, 219, 251(e)(3), 301, 303(b), 303(g), 303(j), 303(r), 307, 309(a), 316, 332, 403, 405, 615a-1, 615c, 621(b)(3), and 621(d) of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154(i), 154 (j), 154 (o), 155(c), 201(b), 214(d), 218, 219, 251(e)(3), 301, 303(b), 303(g), 303(j), 303(r), 307, 309(a), 316, 332, 403, 405, 615a-1, 615c, 621(b)(3), and 621(d) unless otherwise noted.

SOURCE: 72 FR 37673, July 11, 2007, unless otherwise noted.

§12.1 Purpose.

The rules in this part include requirements that will help ensure the resiliency, redundancy and reliability of communications systems, particularly 911 and E911 networks and/or systems.

§12.3 911 and E911 analyses and reports.

The following entities must analyze their 911 and E911 networks and/or systems and provide a detailed report to the Commission on the redundancy, resiliency, and reliability of those networks and/or systems: Local exchange carriers (LECs), including incumbent LECs (ILECS) and competitive LECs (CLECs); commercial mobile radio service providers required to comply with the wireless 911 rules set forth in §20.18 of this chapter; and interconnected Voice over Internet Protocol (VoIP) service providers. LECs that meet the definition of a Class B company set forth in §32.11(b)(2) of this chapter, non-nationwide commercial mobile radio service providers with no more than 500,000 subscribers at the end of 2001, and interconnected VoIP service providers with annual revenues below the revenue threshold established pursuant to §32.11 of this chapter are exempt from this rule.

(a) The Public Safety and Homeland Security Bureau (PSHSB) has the delegated authority to implement and activate a process through which these reports will be submitted, including the authority to establish the specific data that will be required. Where relevant, 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.

(b) These reports are due 120 days from the date that the Commission or its staff announces activation of the 911 network and system reporting process.

(c) Reports filed under this Part will be presumed to be confidential. These reports will be shared with The National Emergency Number Association, The Association of Public Safety Communications Officials, and The National Association of State 9–1–1 Administrators only pursuant to a protective order. PSHSB has the delegated authority to issue such protective orders. All other access to these reports must be sought pursuant to procedures set forth in 47 CFR 0.461. Notice of any requests for inspection of these reports will be provided to the filers of the reports pursuant to 47 CFR 0.461(d)(3).

[72 FR 37673, July 11, 2007]

§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 all of the elements in paragraph (c)(1)(i) 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) 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 October 15, 2014, 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.

[79 FR 3131, Jan. 17, 2014, as amended at 79 FR 7589, Feb. 10, 2014; 80 FR 10619, Feb. 27, 2015; 80 FR 60552, Oct. 7, 2015]

§ 12.5 Backup power obligations.

(a) *Covered service.* For purposes of this section, a Covered Service is any facilities-based, fixed voice service offered as residential service, including fixed applications of wireless service offered as a residential service, that is not line powered.

(b) *Obligations of providers of a Covered Service to offer backup power.* Providers of a Covered Service shall, at the point of sale for a Covered Service, offer subscribers the option to purchase backup power for the Covered Service as follows:

(1) *Eight hours.* Providers shall offer for sale at least one option with a minimum of eight hours of standby backup power.

(2) *Twenty-four hours.* By February 13, 2019, providers of a Covered Service shall offer for sale also at least one option that provides a minimum of twenty-four hours of standby backup power.

(3) At the provider's discretion, the options in paragraphs (b)(1) and (2) of this section may be either:

(i) A complete solution including battery or other power source; or

(ii) Installation by the provider of a component that accepts or enables the use of a battery or other backup power source that the subscriber obtains separately. If the provider does not offer a complete solution, the provider shall install a compatible battery or other power source if the subscriber makes it available at the time of installation and so requests. After service has been initiated, the provider may, but is not required to, offer to sell any such options directly to subscribers.

(c) *Backup power required.* The backup power offered for purchase under paragraph (b) of this section must include power for all provider-furnished equipment and devices installed and operated on the customer premises that must remain powered in order for the service to provide 911 access.

(d) *Subscriber disclosure.* (1) The provider of a Covered Service shall disclose to each new subscriber at the point of sale and to all subscribers to a Covered Service annually thereafter:

(i) Capability of the service to accept backup power, and if so, the availability of at least one backup power solution available directly from the provider, or after the initiation of service, available from either the provider or a third party. After the obligation to offer for purchase a solution for twenty-four hours of standby backup power becomes effective, providers must disclose this information also for the twenty-four-hour solution;

(ii) Service limitations with and without backup power;

(iii) Purchase and replacement information, including cost;

(iv) Expected backup power duration;

(v) Proper usage and storage conditions, including the impact on duration of failing to adhere to proper usage and storage;

(vi) Subscriber backup power self-testing and -monitoring instructions; and

(vii) Backup power warranty details, if any.

(2) *Disclosure reasonably calculated to reach each subscriber.* A provider of a