6712-01

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 10 and 11

[PS Docket No. 15-91; PS Docket No. 15-94; FCC 16-127]

Wireless Emergency Alerts; Amendments to Rules Regarding the Emergency Alert System

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) adopts revisions to Wireless Emergency Alert (WEA) rules to take advantage of the significant technological changes and improvements experienced by the mobile wireless industry since the passage of the Warning, Alert and Response Network (WARN) Act, and deployment of Wireless Emergency Alerts (WEA) to improve utility of WEA as a life-saving tool. By this action, the Commission adopts rules that will improve Alert Message content in order to help communities communicate clearly and effectively about imminent threats and local crises. It also adopts rules to meet alert originators' needs for the delivery of the Alert Messages they transmit and creates a framework that will allow emergency managers to test, exercise, and raise public awareness about WEA. Through this action, the Commission hopes to empower state and local alert originators to participate more fully in WEA, and to enhance the utility of WEA as an alerting tool.

DATES: Amendments and revisions to §§ 10.280, 10.400, 10.410, 10.430, 10.510, and the addition of § 10.350(c) are effective May 1, 2019. The addition of § 10.480 is effective November 1, 2018. The addition of § 10.441 is effective November 1, 2017. Amendments to § 10.450 are effective [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE

FEDERAL REGISTER]. Removal of § 10.440, and amendments to § 10.350 (section heading and introductory text), § 10.350(b), § 10.520(d), and § 11.45 are effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. Section 10.320(g) contains information collection requirements that have not been approved by the Office of Management and Budget (OMB). The Commission will publish a document in the Federal Register announcing an effective date.

FOR FURTHER INFORMATION CONTACT: James Wiley, Attorney Advisor, Public Safety and Homeland Security Bureau, at (202) 418-1678, or by email at James.Wiley@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Report and Order in PS Docket No. 15-91, No. 15-94, FCC 16-127, released on September 29, 2016. The document is available for download at http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0929/FCC-16-127A1.pdf. The complete text of this document is also available for inspection and copying during normal business hours in the FCC Reference Information Center, Portals II, 445 12th Street SW., Room CY-A257, Washington, DC 20554. 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).

Final Paperwork Reduction Act of 1995 Analysis

This Report and Order adopts new or revised information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13 (44 U.S.C. 3501-3520). The requirements will be submitted to the Office of Management and Budget (OMB) for review under Section 3507 of the PRA. The Commission will publish a separate notice in the Federal

Register inviting comment on the new or revised information collection requirements adopted in this document. In addition, 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), we previously sought specific comment on how the Commission might "further reduce the information collection burden for small business concerns with fewer than 25 employees."

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA) the Commission incorporated an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in the WEA NPRM (80 FR 77289, Dec. 14, 2015). No comments were filed addressing the IRFA regarding the issues raised in the WEA NPRM. Because the Commission amends the rules in this WEA Report and Order, the Commission has included this Final Regulatory Flexibility Analysis (FRFA). This present FRFA conforms to the RFA

A. Need for, and Objectives of, the Rules

2. Today's WEA Report and Order adopts rules to empower alert originators to participate more fully in WEA and to enhance the utility of WEA as an alerting tool. In this WEA Report and Order, we adopt rules that fall into three categories, message content, message delivery, and testing and outreach.

3. Specifically, with respect to message content, we increase the maximum Alert Message length from 90 to 360 characters for 4G-LTE and future networks only. We classify Public Safety Messages as an Alert Message eligible to be issued in connection with any other class of Alert Message. We require Participating Commercial Mobile Service (CMS) Providers to support embedded references, and allow Participating CMS providers to include embedded

references in all Alert Message types for the purpose of an industry-led pilot of this functionality. We also require Participating CMS Providers to support transmission of Spanish-language Alert Messages.

4. With respect to message delivery, we require Participating CMS Providers to narrow their geo-targeting of Alert Messages to an area that best approximates the alert area specified by the alert originator. We require that mobile devices process and display Alert Messages concurrent with other device activity. We also require Participating CMS Providers to log Alert Messages, to maintain those logs for at least 12 months, and to make those logs available upon request.

5. With respect to testing and outreach, we require support for State/Local WEA Tests and encourage emergency managers to engage in proficiency training exercises using alert origination software. We require periodic testing of the broadcast-based backup to the C-interface. Finally, we allow federal, state, local, tribal and territorial entities, as well as non-governmental organizations (NGOs) in coordination with such entities to issue Public Service Announcements (PSAs) aimed at raising public awareness about WEA.

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

6. No commenter raised issues in response to the IRFA included in the WEA NPRM. We conclude that these mandates provide Participating CMS Providers with a sufficient measure of flexibility to account for technical and cost-related concerns. In the event that small entities face unique circumstances that restrict their ability to comply with the Commission's rules, we can address them through the waiver process. We have determined that implementing these improvements to WEA is technically feasible and the cost of implementation is small.

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

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

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

9. Wireless Telecommunications Carriers (except satellite). This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to

provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular phone services, paging services, wireless Internet access, and wireless video services. The appropriate size standard under SBA rules for the category Wireless Telecommunications Carriers (except satellite) is that a business is small if it has 1,500 or fewer employees. Census data for 2012 show that there were 967 firms that operated for the entire year. Of this total, 955 firms had employment of fewer than 1000 employees. Thus under this category and the associated small business size standard, the Commission estimates that the majority of wireless telecommunications carriers (except satellite) are small.

10. Broadband Personal Communications Service. The broadband personal communications services (PCS) spectrum is divided into six frequency blocks designated A through F, and the Commission has held auctions for each block. The Commission initially defined a "small business" for C- and F-Block licenses as an entity that has average gross revenues of $40 million or less in the three previous calendar years. For F-Block licenses, an additional small business size standard for "very small business" was added and is defined as an entity that, together with its affiliates, has average gross revenues of not more than $15 million for the preceding three calendar years. These small business size standards, in the context of broadband PCS auctions, have been approved by the SBA. No small businesses within the SBA-approved small business size standards bid successfully for licenses in Blocks A and B. There were 90 winning bidders that claimed small business status in the first two C-Block auctions. A total of 93 bidders that claimed small business status won approximately 40 percent of the 1,479 licenses in the first auction for the D, E, and F Blocks. On April 15, 1999, the Commission completed the reauction of 347 C-, D-, E-, and F-Block licenses in Auction No. 22. Of the 57

winning bidders in that auction, 48 claimed small business status and won 277 licenses.

11. On January 26, 2001, the Commission completed the auction of 422 C and F Block Broadband PCS licenses in Auction No. 35. Of the 35 winning bidders in that auction, 29 claimed small business status. Subsequent events concerning Auction 35, including judicial and agency determinations, resulted in a total of 163 C and F Block licenses being available for grant. On February 15, 2005, the Commission completed an auction of 242 C-, D-, E-, and F-Block licenses in Auction No. 58. Of the 24 winning bidders in that auction, 16 claimed small business status and won 156 licenses. On May 21, 2007, the Commission completed an auction of 33 licenses in the A, C, and F Blocks in Auction No. 71. Of the 12 winning bidders in that auction, five claimed small business status and won 18 licenses. On August 20, 2008, the Commission completed the auction of 20 C-, D-, E-, and F-Block Broadband PCS licenses in Auction No. 78. Of the eight winning bidders for Broadband PCS licenses in that auction, six claimed small business status and won 14 licenses.

12. Narrowband Personal Communications Service. To date, two auctions of narrowband personal communications services (PCS) licenses have been conducted. For purposes of the two auctions that have already been held, "small businesses" were entities with average gross revenues for the prior three calendar years of $40 million or less. Through these auctions, the Commission has awarded a total of 41 licenses, out of which 11 were obtained by small businesses. To ensure meaningful participation of small business entities in future auctions, the Commission has adopted a two-tiered small business size standard in the Narrowband PCS Second Report and Order. A "small business" is an entity that, together with affiliates and controlling interests, has average gross revenues for the three preceding years of not more than $40 million. A "very small business" is an entity that, together with affiliates and

controlling interests, has average gross revenues for the three preceding years of not more than $15 million. The SBA has approved these small business size standards.

13. Wireless Communications Services. This service can be used for fixed, mobile, radiolocation, and digital audio broadcasting satellite uses. The Commission defined "small business" for the wireless communications services (WCS) auction as an entity with average gross revenues of $40 million for each of the three preceding years, and a "very small business" as an entity with average gross revenues of $15 million for each of the three preceding years. The SBA has approved these definitions.

14. 700 MHz Guard Band Licensees. In 2000, in the 700 MHz Guard Band Order, the Commission adopted size standards for "small businesses" and "very small businesses" for purposes of determining their eligibility for special provisions such as bidding credits and installment payments. A small business in this service is an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $40 million for the preceding three years. Additionally, a very small business is an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $15 million for the preceding three years. SBA approval of these definitions is not required. An auction of 52 Major Economic Area licenses commenced on September 6, 2000, and closed on September 21, 2000. Of the 104 licenses auctioned, 96 licenses were sold to nine bidders. Five of these bidders were small businesses that won a total of 26 licenses. A second auction of 700 MHz Guard Band licenses commenced on February 13, 2001, and closed on February 21, 2001. All eight of the licenses auctioned were sold to three bidders. One of these bidders was a small business that won a total of two licenses.

15. Lower 700 MHz Band Licenses. The Commission previously adopted criteria for

defining three groups of small businesses for purposes of determining their eligibility for special provisions such as bidding credits. The Commission defined a "small business" as an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $40 million for the preceding three years. A "very small business" is defined as an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $15 million for the preceding three years. Additionally, the lower 700 MHz Service had a third category of small business status for Metropolitan/Rural Service Area (MSA/RSA) licenses—"entrepreneur"—which is defined as an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $3 million for the preceding three years. The SBA approved these small size standards. An auction of 740 licenses (one license in each of the 734 MSAs/RSAs and one license in each of the six Economic Area Groupings (EAGs)) commenced on August 27, 2002, and closed on September 18, 2002. Of the 740 licenses available for auction, 484 licenses were won by 102 winning bidders. Seventy-two of the winning bidders claimed small business, very small business or entrepreneur status and won a total of 329 licenses. A second auction commenced on May 28, 2003, closed on June 13, 2003, and included 256 licenses: 5 EAG licenses and 476 Cellular Market Area licenses. Seventeen winning bidders claimed small or very small business status and won 60 licenses, and nine winning bidders claimed entrepreneur status and won 154 licenses. On July 26, 2005, the Commission completed an auction of 5 licenses in the Lower 700 MHz band (Auction No. 60). There were three winning bidders for five licenses. All three winning bidders claimed small business status.

16. In 2007, the Commission reexamined its rules governing the 700 MHz band in the 700 MHz Second Report and Order. An auction of 700 MHz licenses commenced January 24,

2008 and closed on March 18, 2008, which included, 176 Economic Area licenses in the A Block, 734 Cellular Market Area licenses in the B Block, and 176 EA licenses in the E Block. Twenty winning bidders, claiming small business status (those with attributable average annual gross revenues that exceed $15 million and do not exceed $40 million for the preceding three years) won 49 licenses. Thirty three winning bidders claiming very small business status (those with attributable average annual gross revenues that do not exceed $15 million for the preceding three years) won 325 licenses.

17. Upper 700 MHz Band Licenses. In the 700 MHz Second Report and Order, the Commission revised its rules regarding Upper 700 MHz licenses. On January 24, 2008, the Commission commenced Auction 73 in which several licenses in the Upper 700 MHz band were available for licensing: 12 Regional Economic Area Grouping licenses in the C Block, and one nationwide license in the D Block. The auction concluded on March 18, 2008, with 3 winning bidders claiming very small business status (those with attributable average annual gross revenues that do not exceed $15 million for the preceding three years) and winning five licenses.

18. Advanced Wireless Services. AWS Services (1710–1755 MHz and 2110–2155 MHz bands (AWS-1); 1915–1920 MHz, 1995–2000 MHz, 2020–2025 MHz and 2175–2180 MHz bands (AWS-2); 2155–2175 MHz band (AWS-3)). For the AWS-1 bands, the Commission has defined a "small business" as an entity with average annual gross revenues for the preceding three years not exceeding $40 million, and a "very small business" as an entity with average annual gross revenues for the preceding three years not exceeding $15 million. For AWS-2 and AWS-3, although we do not know for certain which entities are likely to apply for these frequencies, we note that the AWS-1 bands are comparable to those used for cellular service and personal communications service. The Commission has not yet adopted size standards for the

AWS-2 or AWS-3 bands but proposes to treat both AWS-2 and AWS-3 similarly to broadband PCS service and AWS-1 service due to the comparable capital requirements and other factors, such as issues involved in relocating incumbents and developing markets, technologies, and services.

19. Broadband Radio Service and Educational Broadband Service. Broadband Radio Service systems, previously referred to as Multipoint Distribution Service (MDS) and Multichannel Multipoint Distribution Service (MMDS) systems, and "wireless cable," transmit video programming to subscribers and provide two-way high speed data operations using the microwave frequencies of the Broadband Radio Service (BRS) and Educational Broadband Service (EBS) (previously referred to as the Instructional Television Fixed Service (ITFS)). In connection with the 1996 BRS auction, the Commission established a small business size standard as an entity that had annual average gross revenues of no more than $40 million in the previous three calendar years. The BRS auctions resulted in 67 successful bidders obtaining licensing opportunities for 493 Basic Trading Areas (BTAs). Of the 67 auction winners, 61 met the definition of a small business. BRS also includes licensees of stations authorized prior to the auction. At this time, we estimate that of the 61 small business BRS auction winners, 48 remain small business licensees. In addition to the 48 small businesses that hold BTA authorizations, there are approximately 392 incumbent BRS licensees that are considered small entities. After adding the number of small business auction licensees to the number of incumbent licensees not already counted, we find that there are currently approximately 440 BRS licensees that are defined as small businesses under either the SBA or the Commission's rules.

20. In 2009, the Commission conducted Auction 86, the sale of 78 licenses in the BRS areas. The Commission offered three levels of bidding credits: (i) a bidder with attributed

average annual gross revenues that exceed $15 million and do not exceed $40 million for the preceding three years (small business) received a 15 percent discount on its winning bid; (ii) a bidder with attributed average annual gross revenues that exceed $3 million and do not exceed $15 million for the preceding three years (very small business) received a 25 percent discount on its winning bid; and (iii) a bidder with attributed average annual gross revenues that do not exceed $3 million for the preceding three years (entrepreneur) received a 35 percent discount on its winning bid. Auction 86 concluded in 2009 with the sale of 61 licenses. Of the ten winning bidders, two bidders that claimed small business status won 4 licenses; one bidder that claimed very small business status won three licenses; and two bidders that claimed entrepreneur status won six licenses.

21. In addition, the SBA's Cable Television Distribution Services small business size standard is applicable to EBS. There are presently 2,436 EBS licensees. All but 100 of these licenses are held by educational institutions. Educational institutions are included in this analysis as small entities. Thus, we estimate that at least 2,336 licensees are small businesses. Since 2007, Cable Television Distribution Services have been defined within the broad economic census category of Wired Telecommunications Carriers; that category is defined as follows: "This industry comprises establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies." The SBA has developed a small business size standard for this category, which is: all such firms having 1,500 or fewer employees. To gauge small business prevalence for these cable services we must, however, use the most current census data that are based on the previous category of Cable and

Other Program Distribution and its associated size standard; that size standard was: all such firms having $13.5 million or less in annual receipts. According to Census Bureau data for 2007, there were a total of 996 firms in this category that operated for the entire year. Of this total, 948 firms had annual receipts of under $10 million, and 48 firms had receipts of $10 million or more but less than $25 million. Thus, the majority of these firms can be considered small. In the Paging Third Report and Order, we developed a small business size standard for "small businesses" and "very small businesses" for purposes of determining their eligibility for special provisions such as bidding credits and installment payments. A "small business" is an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $15 million for the preceding three years. Additionally, a "very small business" is an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $3 million for the preceding three years. The SBA has approved these small business size standards. An auction of Metropolitan Economic Area licenses commenced on February 24, 2000, and closed on March 2, 2000. Of the 985 licenses auctioned, 440 were sold. Fifty-seven companies claiming small business status won. Also, according to Commission data, 365 carriers reported that they were engaged in the provision of paging and messaging services. Of those, we estimate that 360 are small, under the SBA-approved small business size standard.

22. Wireless Communications Service. This service can be used for fixed, mobile, radiolocation, and digital audio broadcasting satellite uses. The Commission established small business size standards for the wireless communications services (WCS) auction. A "small business" is an entity with average gross revenues of $40 million for each of the three preceding years, and a "very small business" is an entity with average gross revenues of $15 million for each of the three preceding years. The SBA has approved these small business size standards.

The Commission auctioned geographic area licenses in the WCS service. In the auction, there were seven winning bidders that qualified as "very small business" entities, and one that qualified as a "small business" entity.

23. Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing. This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment. Examples of products made by these establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, and radio and television studio and broadcasting equipment. The Small Business Administration has established a size standard for this industry of 750 employees or less. Census data for 2012 show that 841 establishments operated in this industry in that year. Of that number, 819 establishments operated with less than 500 employees. Based on this data, we conclude that a majority of manufacturers in this industry is small.

24. Software Publishers. Since 2007 these services have been defined within the broad economic census category of Custom Computer Programming Services; that category is defined as establishments primarily engaged in writing, modifying, testing, and supporting software to meet the needs of a particular customer. The SBA has developed a small business size standard for this category, which is annual gross receipts of $25 million or less. According to data from the 2007 U.S. Census, there were 41,571 establishments engaged in this business in 2007. Of these, 40,149 had annual gross receipts of less than $10,000,000. Another 1,422 establishments had gross receipts of $10,000,000 or more. Based on this data, the Commission concludes that the majority of the businesses engaged in this industry are small.

25. NCE and Public Broadcast Stations. The Census Bureau defines this category as

follows: "This industry comprises establishments primarily engaged in broadcasting images together with sound. These establishments operate television broadcasting studios and facilities for the programming and transmission of programs to the public." The SBA has created a small business size standard for Television Broadcasting entities, which is: such firms having $13 million or less in annual receipts. According to Commission staff review of the BIA Publications, Inc., Master Access Television Analyzer Database as of May 16, 2003, about 814 of the 1,220 commercial television stations in the United States had revenues of $12 (twelve) million or less. We note, however, that in assessing whether a business concern qualifies as small under the above definition, business (control) affiliations must be included. Our estimate, therefore, likely overstates the number of small entities that might be affected by our action, because the revenue figure on which it is based does not include or aggregate revenues from affiliated companies.

26. In addition, an element of the definition of "small business" is that the entity not be dominant in its field of operation. We are unable at this time to define or quantify the criteria that would establish whether a specific television station is dominant in its field of operation. Accordingly, the estimate of small businesses to which rules may apply do not exclude any television station from the definition of a small business on this basis and are therefore over-inclusive to that extent. Also as noted, an additional element of the definition of "small business" is that the entity must be independently owned and operated. We note that it is difficult at times to assess these criteria in the context of media entities and our estimates of small businesses to which they apply may be over-inclusive to this extent. There are also 2,117 low power television stations (LPTV). Given the nature of this service, we will presume that all LPTV licensees qualify as small entities under the above SBA small business size standard.

27. The Commission has, under SBA regulations, estimated the number of licensed NCE television stations to be 380. We note, however, that, in assessing whether a business concern qualifies as small under the above definition, business (control) affiliations must be included. Our estimate, therefore, likely overstates the number of small entities that might be affected by our action, because the revenue figure on which it is based does not include or aggregate revenues from affiliated companies. The Commission does not compile and otherwise does not have access to information on the revenue of NCE stations that would permit it to determine how many such stations would qualify as small entities.

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

28. In the WEA Report and Order, we amend our Part 10 rules for Participating CMS Providers, as defined in the WEA rules, to require them to create and maintain logs of Alert Messages received at their Alert Gateway from FEMA IPAWS, and to make available to emergency management agencies information about the measures they take to geo-target Alert Messages transmitted by that agency.

29. We consider compliance costs associated with the alert logging and geo-targeting disclosure rules that we adopt today to be reporting and recordkeeping costs. These costs include a one-time expense to establish the Alert Gateway logging capability for the few Participating CMS Providers that may not already have this capability, and the small, annual expense of automatically generating and maintaining alert logs, and the potentially larger expense of the employment of a clerical worker to respond to emergency management agencies' requests for alert log data or requests for information about geo-targeting. These alert logging and reporting requirements represent a somewhat more lenient version of the alert logging requirements we

proposed in the WEA NPRM. To the extent these costs may still present a burden to non-nationwide Participating CMS Providers, we offer such entities an extended timeframe for compliance with our alert logging requirement in order to allow them to standardize appropriate gateway behavior and integrate any updates into their regular technology refresh cycle.

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

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

31. The compliance requirements in this WEA Report and Order have been adjusted to accommodate the special circumstances of non-nationwide Participating CMS Providers with respect to our WEA geo-targeting requirements and our alert logging requirements. According to the Annual Competition Report, "there are four nationwide providers in the U.S. with networks that cover a majority of the population and land area of the country – Verizon Wireless, AT&T, Sprint, and T-Mobile." Consistent with the Annual Competition Report, we refer to other providers with "networks that are limited to regional and local areas" as non-nationwide Participating CMS Providers. We allow non-nationwide Participating CMS Providers one year within which to comply with our WEA geo-targeting rules and two years to comply with our

alert logging rules, instead of sixty days from the rules' publication in the Federal Register, in light of a non-nationwide Participating CMS Provider's inability to meet that standard immediately, and our concern that other non-nationwide Participating CMS Providers may be similarly situated. We believe that applying the same rules equally to all entities in this context is not necessary to alleviate potential confusion from adopting different rules for Participating CMS Providers because most consumers do not have insight into the relative accuracy of various Participating CMS Providers geo-targeting capabilities, and because alert logging is not a consumer facing service. We believe, and the record in this proceeding confirms, that the costs and/or administrative burdens associated with the rules will not unduly burden small entities, particularly in light of the special consideration we provide to them. These requirements will implicate no additional legal concerns, and will require no additional professional assistance for non-nationwide Participating CMS Providers.

32. Based on our review of the record, we find that it is practicable for all Participating CMS Providers, including non-nationwide Participating CMS Providers, to implement WEA improvements without incurring unduly burdensome costs, especially considering the special treatment that we afford non-nationwide Participating CMS Providers. The WEA Report and Order recognizes that technical and operational issues must be addressed before compliance can be required, and allows sufficient time for nationwide and non-nationwide Participating CMS Providers to achieve compliance with today's rules.

33. In considering the record received in response to the WEA NPRM, we examined additional alternatives to ease the burden on non-nationwide EAS Participants. These alternatives included adopting longer compliance timeframes than those initially proposed; requiring Participating CMS Providers to support WEA Alert Messages that contain only360

characters, as opposed to 1,380, as considered by the Updated START Report; requiring support for only additional languages that are currently supported by standards, as opposed to others as initially proposed; and allowing Participating CMS Providers geo-target an Alert Message to an area that "best approximates" the target area, as opposed to one that is "no larger than" the target area using device-based geo-fencing techniques, as proposed. Additionally, the rules adopted in this WEA Report and Order are technologically neutral in order to enable small entities flexibility to comply with our rules using technologies offered by a variety of vendors. Finally, we sought further comment on some issues where the record demonstrated that it would be premature to adopt rules at this time, particularly for non-nationwide CMS Providers.

34. Finally, in the event that small entities face unique circumstances with respect to these rules, such entities may request waiver relief from the Commission. Accordingly, we find that we have discharged our duty to consider the burdens imposed on small entities.

F. Legal Basis

35. The legal basis for the actions taken pursuant to this WEA Report and Order is contained in 47 U.S.C. 151, 152, 154(i) and (o), 301, 301(r), 303(v), 307, 309, 335, 403, 544(g), 606 and 615 of the Communications Act of 1934, as amended, as well as by sections 602(a), (b), (c), (f), 603, 604 and 606 of the WARN Act.

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

36. None

H. Congressional Review Act

37. The Commission will send a copy of this Report & Order to Congress and the Government Accountability Office pursuant to the Congressional Review Act, see 5 U.S.C. 801(a)(1)(A).

Synopsis

I. REPORT AND ORDER

A. Alert Message Content

1. Increasing Maximum Alert Message Length from 90 to 360 Characters

38. We amend Section 10.430 to expand the character limit for Alert Messages from 90 to 360 characters for 4G-LTE and future networks. A 360-character maximum Alert Message length balances emergency managers' needs to communicate more clearly with their communities with the technical limitations of CMS networks. While Hyper-Reach states that support for "1,000+" characters would be preferable because it would be consistent with the START Report's findings that messages longer than 1,380 characters produce "better outcomes for interpretation, personalization and milling, than did the standard 90-character WEA message," this approach is not supported by the weight of the record. Beaufort County cautions, for example, that "people will stop reading" Alert Messages once they get past the second screen of text, diminishing the value of any additional characters that extend beyond that, and moreover, longer Alert Messages may contribute to distracted driving. On balance, we find that a 360-character maximum for Alert Message text "is appropriate for disseminating official, targeted, immediate, and actionable information." We note that establishing 360 characters as the maximum character length leaves emergency managers free to issue Alert Messages that are shorter than 360 characters in appropriate situations. We defer to emergency managers' experience and best practices to determine the appropriate message length for their particular needs.

39. We also find that expanding the maximum character length to 360 for 4G-LTE

networks is technically feasible. As we observed in the WEA NPRM, CSRIC IV recommended that the Commission expand the character limit for WEA Alert Messages on 4G LTE networks to a maximum of 280 characters, pending confirmation by the Alliance for Telecommunications Industry Solutions (ATIS) that such an increase would be feasible. Not only did ATIS' feasibility study conclude that it was feasible for 4G-LTE networks to transmit 280-character WEA Alert Messages, but it found that Participating CMS Providers could transmit 360-character Alert Messages just as easily. ATIS found that transmission of WEA Alert Messages longer than 360 characters, on the other hand, would cause additional delays in the delivery of the Alert Message and could drain battery life. Commenting Participating CMS Providers and device manufacturers agree. In addition to the feasible steps that compliance with this rule will require Participating CMS Providers to take, FEMA states that the increased message length will require "software modifications to CAP message authoring tools, IPAWS OPEN, [and] the 'C' Interface." We find that we can achieve our goal of expanding the maximum character limit for WEA Alert Messages on 4G-LTE networks without presenting WEA stakeholders with undue technical burdens.

40. We also find, however, that we should continue to allow Participating CMS Providers to transmit 90-character Alert Messages on legacy networks until those networks are retired. While many public safety commenters, including APCO and Harris County OSHEM, state that it would be feasible and desirable to support 360-character Alert Messages on legacy networks by linking together (concatenating) multiple 90-character messages, we are convinced by AT&T that message concatenation would be problematic because "[m]essages are not guaranteed to be received by the device in the correct order," which would likely cause confusion that would be exacerbated during the pendency of multiple alerts. Further, according

to AT&T, concatenating 90-character Alert Messages on legacy networks would have an adverse effect on mobile device battery life. T-Mobile, Sprint and Microsoft agree that, unlike 4G-LTE networks, it would be infeasible to expand the character limit for legacy networks due to the technical limitations of those networks, and because of financial disincentives to continue to update networks that will soon be retired. The risks that public confusion and other complications would result from Alert Message concatenation are too great for public safety messaging where the potential for panic is heightened, and the consequences of misinterpretation could be deadly.

41. Emergency managers will be free to transmit an Alert Message containing as many as 360 characters as of the rules' implementation date. FEMA IPAWS will make this possible, while also ensuring that all community members in the target area, including those on legacy networks, can receive an Alert Message, by automatically generating a 90-character Alert Message from the CAP fields of a 360-character message for distribution on legacy networks whenever an emergency manager transmits only a 360-character Alert Message. Once a CMS network is able to support 360-character messages, it will cease to receive the 90-character version, and begin to receive the full 360-character version instead. CSRIC IV and FEMA attest that this co-existence of 90- and 360-character Alert Messages is technically feasible. Indeed, FEMA IPAWS already treats Alert Messages that do not contain free-form text in this manner, and their approach is consistent with the methodology that the Participating CMS Provider Alert Gateway will use to process Alert Messages in multiple languages. For example, if FEMA IPAWS receives an Alert Message today without free-form text, it will use the CAP parameters [hazard][location][time][guidance][source] to generate Alert Message text along the lines of "Tornado Warning in this area until 6:30 PM. Take Shelter. Check Local Media. –NWS." The

CMS Provider Alert Gateway will send the longer free-form message to devices on 4G-LTE networks, and the automatically generated 90-character Alert Message to mobile devices on legacy networks. Pursuant to the approach we adopt today, no matter how an alert originator transmits a WEA Alert Message, members of their community in the target area will receive a version of it.

42. Increasing the maximum character length for WEA Alert Messages will produce valuable public safety benefits. Emergency managers state that the current 90-character limit is insufficient to communicate clearly with the public because 90-character Alert Messages rely on difficult-to-understand jargon and abbreviations. Expanding the character limit will reduce reliance on these potentially confusing terms and will allow emergency managers to provide their communities with information that is clear and effective at encouraging swift protective action. The value of this benefit will be increased when taken together with several of the improvements that we adopt in this Report and Order. For example, according to Jefferson Parish Emergency Management, the additional characters are necessary to adequately communicate critical information, such as shelter locations, that could prevent unnecessary loss of life and property damage. The additional characters will also support the inclusion of embedded references in Alert Messages, help facilitate message comprehension for individuals with disabilities, and will facilitate the translation of English-language Alert Messages into the Spanish language. Further, our approach to the co-existence of 90- and 360-character Alert Messages has the additional benefit of ensuring that emergency managers will be able to simply initiate one 360-character Alert Message in instances where every second counts. In sum, this action will improve the likelihood that the public will understand and properly respond to WEA Alert Messages, increasing the likelihood that WEA will save lives.

2. Establishment of a New Alert Message Classification (Public Safety Messages)

43. We amend Section 10.400 to create a fourth classification of Alert Message, "Public Safety Message." The current rules only provides for three classes of WEA: (1) Presidential Alert; (2) Imminent Threat Alert; and (3) AMBER Alert. For an alert originator to issue an Alert Message using WEA, it must fall within one of these three classifications. Whereas we proposed to name this new Alert Message classification "Emergency Government Information" in the WEA NPRM, we agree with FEMA that it should be named "Public Safety Message" because the title "Emergency Government Information" is "vague and could be confusing," and because FEMA's recommended title more accurately describes the intended message content. We define a Public Safety Message as "an essential public safety advisory that prescribes one or more actions likely to save lives and/or safeguard property," as we proposed. By defining Public Safety Messages in this way and by tailoring their use as we describe below, we strike an appropriate balance between some commenters' requests for discretion in the use of this new Alert Message classification, and others' warnings that Public Safety Messages may be overused and contribute to alert fatigue if they are defined in an over-inclusive manner.

44. Public Safety Messages will only be eligible for issuance in connection with an Imminent Threat Alert, an AMBER Alert, or a Presidential Alert, as recommended by AT&T, CTIA and several emergency management agencies. We do not expand the definition of an "emergency" situation in which it is appropriate to issue an Alert Message so as to avoid alert fatigue. Instead, we add a tool for emergency managers to better communicate with the public during and after emergencies, in a manner that naturally complements existing Alert Message classifications. We note that several commenters state that our new Alert Message classification

should be eligible for issuance even in the absence of another Alert Message type. If we were to allow Public Safety Messages to stand alone, however, it would expand the definition of an "emergency" during which the issuance of a WEA Alert Message is appropriate, contrary to our reasoning in the WEA First Report and Order that the existing Alert Message classifications are sufficient to communicate information about "bona fide emergencies." Further, we believe that a broader definition of an "emergency" would risk increasing alert fatigue and consumer opt out.

45. Any entity authorized to use WEA may initiate Public Safety Messages. Some commenters state that we should limit eligibility to issue Public Safety Messages to government entities. This may be because it would not make sense for non-governmental entities to issue Alert Messages under our proposed title, "Emergency Government Information." Moreover, we agree with the majority of emergency managers treating the issue that all entities that have completed FEMA IPAWS alert originator authorization process may send Public Safety Messages. We thus defer to FEMA, as we have done since WEA's deployment, to determine the suitability of agencies as WEA alert originators.

46. Within this framework, we agree with commenters that the development of best practices around the use of Public Safety Messages will help ensure that this new Alert Message classification is used appropriately. NYCEM offers a number of best practices that would help inform emergency managers' determination of whether it is appropriate to send a Public Safety Message. These best practices include answering the following questions prior to initiating a Public Safety Message: "'Is your emergency operations center activated?' 'Has a competent, authorized party declared a state of emergency and/or are emergency orders being issued?' 'Is there a need for broad public action or awareness of a condition that is occurring or likely to occur?' 'Will the message prevent public fear or serve to preserve critical public safety

functions that are (or could be) overwhelmed (e.g., inappropriate use of 911)?'" We encourage emergency management agencies to build upon these best practices and incorporate them into any alert origination training modules that they may develop for their staff. We expect that emergency managers will be best positioned to determine the specific situations in which it is appropriate to issue Public Safety Messages. We will monitor the use of this new Alert Message classification, and will take further action in the event it becomes evident that our adopted definition is either too narrow or too broad.

47. We do not agree with commenters that, rather than create a new Alert Message classification, we should clarify that the types of Alert Messages that would be issued as Public Safety Messages can be issued as Imminent Threat Alerts. The term "Imminent Threat Alert" is defined in our rules as "an alert that meets a minimum value for each of three CAP elements: Urgency, Severity, and Certainty." Public Safety Messages would not fit within this definition because the "severity" and "urgency" elements of an Imminent Threat Alert describe the underlying imminently threatening emergency condition, whereas Public Safety Messages are intended to provide supplemental instructions about how to protect life or property during an AMBER Alert, Presidential Alert, or Imminent Threat Alert. We anticipate that this separate and broader applicability for Public Safety Messages will make them more versatile emergency management tools than if we were to limit such Alert Messages to the preexisting definition of an Imminent Threat Alert.

48. In addition to tailoring the scope of emergency managers' use of Public Safety Messages, we also take steps to ensure that the public receives Public Safety Messages in an appropriate manner. Specifically, we amend Section 10.280 to specify that Participating CMS Providers shall provide for their subscribers to receive Public Safety Messages by default, and

may provide their subscribers with the option to opt out of receiving Public Safety Messages if they decide that they no longer wish to receive them. We agree with the majority of commenters that the public should be opted in to receiving Public Safety Messages by default because the information that they provide is essential by definition. We agree with Hyper-Reach that treating Public Safety Messages in this manner ensures that a greater percentage of the public will receive the information that Public Safety Messages are intended to provide than would be possible if the public were opted out of receiving Public Safety Messages by default.

49. Further, we allow, but do not require Participating CMS Providers to associate a unique attention signal or vibration cadence with Public Safety Messages. We agree with ATIS that requiring a new, unique attention signal and vibration cadence could create "significant technical impacts" for currently deployed WEA-capable mobile devices. We also agree with FEMA, however, that "the option to silence alerts that do not present an immediate threat" may have value in reducing consumer opt out. By allowing Participating CMS Providers to offer this functionality, we allow the market to determine whether or not any costs that may be implicated by these personalization options are outweighed by the benefits. Similarly, we will allow, but do not require Participating CMS Providers to provide their customers with the ability to turn off Public Safety Messages during certain hours. For example, if customers want to receive Public Safety Messages, but only during the daytime, they may be given the option to suppress the presentation of Public Safety Messages during nighttime hours.

50. APCO and many emergency management agencies support our creation of a new Alert Message classification because it "will enable public safety alert originators to take advantage of WEA when helpful, as compared to less secure and less immediate methods they may be employing presently." We agree with commenters that adding a new Alert Message

classification will allow emergency managers to expand their "capabilities of informing the public . . . to keep the residents and community safe and aware of potential situations" during and after emergencies in a manner that complements existing Alert Message classifications. We also agree with Peoria County EMA that a new classification of Alert Messages would allow emergency managers to include specific secondary information, like shelter locations and other helpful disaster recovery instructions in WEA for the first time. Finally, we agree with commenters and CSRIC IV that it is technically feasible to support the transmission of this new Alert Message classification provided the sufficient time that we allow industry to update relevant standards.

3. Supporting Embedded References and Multimedia

51. We require Participating CMS Providers to support embedded references, as proposed. Accordingly, Participating CMS Providers must support the transmission of embedded URLs and phone numbers in WEA Alert Messages. This rule will become effective one year from the rules' publication in the Federal Register. Further, thirty days from the date the rules are published in the Federal Register, we allow voluntary, early adoption of embedded references through an industry-established and industry-led pilot program. With respect to multimedia, we find that the inclusion of multimedia capability in WEA Alert Messages can result in tremendous public safety benefits. At the same time, however, we recognize that additional standards development remains necessary. Accordingly, we seek comment in the Further Notice regarding the establishment of an appropriate regulatory framework and timeframe for incorporating multimedia capability into WEA Alert Messages. In order to facilitate the development of standards for multimedia in the swiftest timeframe possible, we allow voluntary, early prototyping of certain multimedia capabilities in Public Safety Messages

30 months from the effective date of the rules, as described in greater detail below.

52. Participating CMS Providers express concern that allowing embedded references in Alert Messages would risk network congestion, but the weight of the record supports our conclusion that this action will be more likely to reduce network loading than to increase it. The public already accesses public safety and other resources using the data network upon receipt of WEA messages that do not include embedded references. This behavior, known as "milling," is a predictable public response to receiving an Alert Message, as members of the public will seek to confirm that the indicated emergency condition is indeed occurring, and to gather additional information not provided by the Alert Message to inform their response. Milling is considered undesirable from a public safety perspective because it increases the delay between receiving an Alert Message and taking an appropriate protective action, and from a network management perspective because it increases use of the data network. We agree with FEMA, the National Weather Service (NWS), NYCEM, Dennis Mileti, Professor Emeritus of Sociology at The University of Colorado, and the many emergency managers treating this issue that providing access to additional text and resources through URLs embedded in WEA Alert Messages could actually reduce network congestion by channeling the public's milling behavior through a single authoritative and comprehensive resource. This finding is also supported by the 2014 and 2015 START Reports, which state that providing the public with access to enhanced information in WEA Alert Messages can help to convince people to take protective action more quickly. Upon review of these studies and expert analyses, we are persuaded that embedded references are likely to reduce network load when included in Alert Messages.

53. Finally, Participating CMS Providers who claim that embedded references will result in harmful network congestion have offered no network models, or any other form of

rigorous network analysis, to support their proposition that allowing embedded references in WEA would cause or contribute to network congestion. While all network activity contributes to network congestion to some degree, the unsupported assertion of a risk of network congestion cannot be the sole basis for declining to adopt any measure that utilizes the data network, particularly a measure that has been demonstrated to have a statistically significant impact on WEA's ability to save lives. In the absence of data to the contrary, and in light of the significant record outlined above, we conclude that even if support for embedded references were to result in an incremental increase in data network usage in some cases, this increase would be insufficient to affect network performance during emergencies. Further, we observe that many WEA-capable mobile devices are set to offload network usage to Wi-Fi where available by default, and nearly all smartphones make this option available through the settings menu. Thus, many individuals who choose to click on an embedded reference will not use the mobile data network to access them at all.

54. At the same time, however, we seek to ensure that Participating CMS Providers are able to assess the performance of their networks in real-world conditions and have an opportunity to make any necessary adjustments to accommodate embedded references. AT&T and CCA support "moving ahead with a time-limited trial on their wireless network for purposes of determining whether embedded URLs result in unmanageable congestion when included in Amber Alerts." We therefore allow voluntary, early adoption of embedded references through an industry-established and industry-led pilot. In this regard, we allow Participating CMS Providers, if they choose, to "pressure test" the use of embedded references in Alert Messages in a sample of their network area or subscriber base, prior to full implementation. To this end, Participating CMS Providers may voluntarily coordinate with NCMEC, NWS, FEMA, and other

stakeholders to accomplish a targeted, pilot deployment of embedded references in WEA in a particular geographic location, Alert Message classification, or to a particular subset of subscribers thirty days from the rule's publication in the Federal Register, and prior to the effective date of our rule requiring support for embedded references. We encourage all WEA alert initiators to work with Participating CMS Providers as this functionality is piloted and deployed in order to establish best practices for the inclusion of embedded references in Alert Messages, including the development of any network congestion mitigation strategies as appropriate. For example, stakeholders could voluntarily agree to constrain the amount of data that is made available through an embedded reference. We note that NCMEC already states that it intends to use a low-bandwidth (15kB or less), mobile-friendly version of their website (missingkids.com) in connection with their issuance of WEA AMBER Alerts. C Spire, FEMA and NWS have suggested that limiting the bandwidth requirements of embedded references will likely mitigate the risk of network congestion by limiting the amount of data that will need to be transferred. We defer to Participating CMS Providers to identify the specific terms and timeframe of any such pilot deployment on their own initiative, as well as to undertake any necessary coordination, whether they do so individually or through a third-party coordinator of their choosing.

55. CSRIC IV and FEMA agree that support for embedded references in alert origination software, IPAWS, the C-interface, and on mobile devices can be enabled through a straightforward process of updating standards and software. The successful use of embedded references will also require the development of appropriate best practices. Specifically, CSRIC IV observes that some individuals, particularly those with feature phones, may not have access to the data connection necessary to access content made available by URLs. We share this concern,

and urge emergency managers to continue to convey the most important actionable information through the Alert Message text to ensure that all members of the public are able to receive that information, even if they are unable to access the URL. Commenters also express concern that inadequately prepared web servers or call centers may become overloaded as a result of mass access. NCMEC assures us that the AMBER Alerts website is capable of handling the expected increase in traffic, and we urge all alert originators to take appropriate steps to ensure the preparedness of their web hosting service before initiating an Alert Message that contains a URL. Further, we urge emergency managers to consider the capacity of their call centers or hotlines before embedding a phone number in an Alert Message.

56. Finally, commenters express concern that allowing embedded references in Alert Messages may provide an opportunity for a malicious actor to compromise WEA. To the extent that Participating CMS Providers take part in this opportunity to pilot the use of embedded references in WEA Alert Messages, they should take appropriate steps, in concert with their pilot program partners, to ensure the integrity of the embedded references they transmit. We also encourage emergency management agencies to continue to work with FEMA and Participating CMS Providers to ensure the authenticity and integrity of every Alert Message they initiate. For example, NCMEC confirms that it already authenticates the content on every AMBER Alert on its website and that it will take measures to ensure the security of any URL that it might embed in a WEA AMBER Alert. We note that all WEA Alert Messages are protected with a CAP digital signature that effectively prevents malicious intrusion into Alert Message content in transit. We also note that industry has already begun to take steps to address any particular cybersecurity issues that may be implicated by allowing URLs to be included in WEA. Pursuant to the recommendation of CSRIC V, ATIS is completing a best practice standard to address

potential threat vectors for WEA, including embedded references. We also encourage Participating CMS Providers and alert originators to work with FEMA to develop protocols that may help to mitigate potential risks.

57. Commenters identify the inclusion of embedded references in Alert Messages as the most critical among all of our proposed improvements to WEA. NCMEC, in particular, has found this capability to be paramount to the success of AMBER Alerts. We agree that allowing emergency managers to embed URLs in Alert Messages empowers them to offer the public multimedia-capable, comprehensive emergency response resources. Including an authoritative URL will also likely lead to swifter community response by reducing the likelihood that consumers will seek to verify information through additional sources before taking action. We also agree with commenters that allowing URLs to be included in Alert Messages will improve WEA accessibility, could streamline the public's use of 911 services, and would provide alert originators with a method to ensure the public has access to up-to-date information.

58. In addition to embedded URLs, allowing embedded phone numbers to be included in Alert Messages will offer the public significant public safety benefits. We agree with emergency managers, disability rights advocates and individuals that support including phone numbers in Alert Messages because integrating clickable phone numbers into WEA will provide an accessible method to quickly contact public safety officials. This capability may be particularly relevant to WEA AMBER Alerts where emergency management organizations will often establish special hotlines or call centers to receive reports about missing children that may be reached at a phone number other than 911 that may not be as commonly known. According to FEMA, providing the public with a direct emergency telephone number could hasten emergency response, and help to ensure that calls to 911 will not have to be rerouted. In sum,

allowing embedded references to be included in WEA Alert Messages will dramatically improve WEA's effectiveness at moving the public to take protective action.

59. With respect to multimedia, our decision to require support for embedded references in WEA Alert Messages is an important first step towards ensuring that WEA can be used to provide the public with actionable multimedia content during emergencies. The record shows that WEA's effectiveness depends on its ability to help the all members of the public to close the thought-action gap, and that including multimedia content in Alert Messages themselves would hasten protective action taking, reduce milling, and improve Alert Message accessibility. We therefore believe that support for multimedia content has the potential to provide tremendous public safety benefits and should be implemented as soon as technically feasible. Recognizing that further standards development remains necessary to integrate multimedia technology into WEA, we seek comment in the Further Notice on how best to implement the support of multimedia content in WEA Alert Messages in a reasonable timeframe. In particular, as described in greater detail in the Further Notice, we seek comment on the inclusion of thumbnail-sized images, including hazard symbols, in Public Safety Messages on 4G LTE and future networks. In the interim, in order to facilitate the swift development of standards for supporting multimedia content in WEA, we allow the industry to participate in voluntary prototyping of this functionality in Public Safety Messages, in coordination with FEMA, emergency management agencies, and other relevant WEA stakeholders, as of the effective date of our rule requiring support for Public Safety Messages.

4. Supporting Spanish-language Alert Messages

60. We adopt a new Section 10.480 requiring Participating CMS Providers to support the transmission of Spanish-language Alert Messages. This, along with Section 10.500(e) of the

Commission's WEA rules, which requires "extraction of alert content in English or the subscriber's preferred language," will provide a framework to ensure that Spanish-language Alert Messages will be processed and displayed properly. Pursuant to this framework, we would expect that Spanish-language WEA Alert Messages would be displayed on and only on WEA-capable mobile devices where the subscriber has specified Spanish as their preferred language.

61. The record demonstrates that it is technically feasible for Participating CMS Providers to support Spanish-language Alert Messages. ATIS has developed standards that support the Alert Gateway, the CMS Provider network and mobile devices in receiving, transmitting and displaying Alert Messages in Spanish as well as English. We applaud ATIS for completing these standards, and encourage their continued efforts to standardize network functionality for Alert Messages in additional languages. According to Microsoft, multilingual alerting is already taking place in other countries.

62. We agree with Participating CMS Providers that they should not be responsible for Alert Message translation. Rather, emergency managers are the entities best equipped to determine message content, including content in other languages. We recognize that some emergency management agencies report that they do not currently have the capability to initiate Alert Messages in languages other than English. Other emergency management agencies, such as Harris County OHSEM, state that they do have this capability, and "NYCEM is in the final stages of preparing to offer . . . [its] 80 most common messages in the 13 most commonly spoken languages in New York City, including American Sign Language," but those messages would have to be transmitted using alternative alerting platforms until WEA's multilingual alerting capabilities improve.

63. We anticipate that requiring Participating CMS Providers to support Spanish-

language Alert Messages where available will encourage other emergency management agencies to continue to develop their multilingual alerting capabilities. Indeed, many emergency managers state that they can use State/Local WEA Tests as a tool to exercise and improve their multilingual alerting capability over time with the help of voluntary community feedback. We do not agree with NYCEM and Clark County OEM, however, that we should facilitate Alert Message translation by requiring Participating CMS Providers to "place a 'translate' button/link" in WEA Alert Messages. Rather, we agree with FEMA and the majority of emergency management agencies that automatic translation technologies that may reside on some mobile devices are currently too inaccurate to support emergency messaging.

64. The overwhelming majority of emergency management agencies support expanding WEA's language capabilities because it will help them to reach members of their communities that are currently inaccessible to them. Emergency managers in areas with large Spanish-speaking populations, as well as those in areas popular among tourists, state that requiring support for Spanish-language WEA Alert Messages will be particularly beneficial. We also anticipate that this action will allow emergency managers to better facilitate the inclusion of Spanish-speaking individuals, and particularly those with limited English proficiency, into their emergency response plans.

B. Alert Message Delivery

1. Logging Alert Messages at the Participating CMS Provider Alert Gateway

65. We require Participating CMS Providers to log their receipt of Alert Messages at their Alert Gateway and to appropriately maintain those records for review. Specifically, we adopt a new Section 10.320(g) that will require Participating CMS Providers' Alert Gateways to

log Alert Messages as described below. Based on the record, we have modified the rules we proposed in the WEA NPRM in order to accommodate the varied approaches Participating CMS Providers take to alert logging.

- Logging Requirements. Participating CMS Providers are required to provide a mechanism to log the CMAC attributes of all Alert Messages received at the CMS Provider Alert Gateway, along with time stamps that verify when the message is received, and when it is retransmitted or rejected by the Participating CMS Provider Alert Gateway. If an alert is rejected, a Participating CMS Provider is required to log the specific error code generated by the rejection.
- Maintenance of Logs. Participating CMS providers are required to maintain a log of all active and cancelled Alert Messages for at least 12 months after receipt of such alert or cancellation.
- Availability of Logs. Participating CMS Providers are required to make their alert logs available to the Commission and FEMA upon request. Participating CMS Providers are also required to make alert logs available to emergency management agencies that offer confidentiality protection at least equal to that provided by the federal Freedom of Information Act (FOIA) upon request, but only insofar as those logs pertain to alerts initiated by that emergency management agency. We encourage, but do not require, Participating CMS Providers to work with alert origination software vendors to automate transmission of alert log data to emergency managers' alert origination software.

66. We find that compliance with these minimal alert logging requirements will be technically feasible. Indeed, the approach we adopt today is a more flexible and less

burdensome alternative to that which we proposed in the WEA NPRM, and allows Participating CMS Providers to take a variety of approaches to achieve compliance. T-Mobile, Verizon, AT&T, Bluegrass Cellular and C Spire already log Alert Messages, and we anticipate that many other Participating CMS Providers may already be doing so as well, as part of their own system maintenance best practices. While Participating CMS Providers have taken different approaches to logging Alert Messages relative to the Trust Model recommended by CMSAAC, we anticipate that those Participating CMS Providers that already do log Alert Messages would log at least the CMAC attributes of all Alert Messages received, and be capable of sending error reports to the FEMA Alert Gateway consistent with those stipulated in the CMSAAC Report. We recognize Verizon's concern that requiring logging of information more granular than CMAC attributes and time stamps, or requiring alert logging at junctures in the WEA system other than the Alert Gateway would "impose burdensome paperwork and IT-related requirements," but the requirements that we adopt today require only basic logging functionality at the Alert Gateway. We also recognize T-Mobile's concern that a uniform system of alert logging would be required in order to aptly compare Participating CMS Provider alert logs. We do not require Participating CMS Providers to take a uniform approach to alert logging today, only that they log the relevant information, maintain that information and make it available to appropriate parties. Further, the CMSAAC Report already stipulates a standard set of error code messages for communication between Participating CMS Provider and FEMA Alert Gateways. Finally, we recognize CTIA's concern about requiring alert logs to be maintained longer than necessary. By requiring alert logs to be maintained for 12 months, rather than 36, as proposed, we reduce the burden that alert log maintenance may pose for Participating CMS Providers. CTIA observes that a shorter alert log maintenance timeframe would incentivize emergency management agencies to request alert

log data after every test or alert out of concern that alert log data may be deleted if they delay. At the same time, however, necessitating emergency management agencies to request logging information after every test is burdensome for both CMS Providers (who must produce this data) and the emergency managers (who must request the data). We believe that requiring that alert logs be retained for one year strikes an appropriate balance that will allow emergency management agencies to request reports less frequently, posing lesser burdens on Participating CMS Providers and emergency management agencies, without requiring providers to retain logs for an extended period of time. Further, circumstances may arise that warrant a retrospective examination of prior log data that represents a sufficient period of time to accurately identify and represent trends or anomalies.

67. Alert logging has been a fundamental aspect of the WEA Trust Model. As we adopt changes to our rules that reflect our four years of experience with WEA and the underlying advancements of technology, it is time to ensure this fundamental component of system integrity is implemented. Authorized WEA alert originators agree that alert logs maintained at the Participating CMS Provider Alert Gateway have potential to increase their confidence that WEA will work as intended when needed. According to emergency managers, this increased confidence in system availability will encourage emergency managers that do not currently use WEA to become authorized. Alert logs are also necessary to establish a baseline for system integrity against which future iterations of WEA can be evaluated. Without records that can be used to describe the quality of system integrity, and the most common causes of message transmission failure, it will be difficult to evaluate how any changes to WEA that we may adopt subsequent to this Report and Order affect system integrity. We disagree with AT&T, Sprint and ATIS that the responsibility for alert logging properly belongs with FEMA IPAWS because

FEMA has access to sufficient information to generate these reports. We find that alert logging is particularly important at Participating CMS Providers' Alert Gateway because even though FEMA IPAWS maintains an alert log at their Alert Gateway as well, that alert log alone could not capture and describe alert delivery across the C-interface, which is arguably the most critical interface in the WEA architecture because it describes the connection between the public aspect of WEA (FEMA IPAWS) and the private aspect (CMS Providers). Additionally, the time stamps that we require Participating CMS Providers to log for Alert Message receipt and retransmission may represent a useful model for collecting latency data throughout the WEA system, as proposed in the Further Notice. As discussed in further detail below, developing a stronger understanding of the extent of alert delivery latency is also crucial to building emergency managers' confidence that the system will work as intended when needed. We anticipate that the alert log maintenance requirements that we adopt today will serve to ensure that alert logs are available when needed, both to the Commission and to emergency management agencies. Indeed, any alert logging requirement would be seriously undermined if those logs could be overwritten as soon as they were recorded, or if they could not be reviewed in appropriate circumstances. Further, we observe that the alert log maintenance requirements that we adopt today are consistent with CMSAAC's initial recommendations for the WEA system. Finally, we observe that implementing these CMSAAC-recommended procedures would be beneficial in harmonizing our WEA logging requirements with those already in place for EAS Participants.

2. Narrowing Geo-targeting Requirements

68. We narrow our WEA geo-targeting requirement from the current county-level standard to a polygon-level standard. Specifically, we amend Section 10.450 to state that a

Participating CMS Provider must transmit any Alert Message that is specified by a geocode, circle, or polygon to an area that best approximates the specified geocode, circle, or polygon. While we initially proposed that Participating CMS Providers should transmit the Alert Message to an area "no larger than" the specified area, the record shows that implementation of such a standard, in the absence of geo-fencing, would routinely and predictably lead to under alerting. We acknowledge, as do many emergency managers, that cell broadcast technology has a limited capacity for accurate geo-targeting. The "best approximates" standard we adopt today, recommended by CSRIC IV and supported by Participating CMS Providers, requires Participating CMS Providers to leverage that technology to its fullest extent, given its limitations. At the same time, as we discuss below, we acknowledge that emergency managers need even more granular geo-targeting than the "best approximates" standard requires. We commend Participating CMS Providers for voluntarily geo-targeting Alert Messages more accurately than our rules require, where possible, in the years since WEA's deployment. We expect that Participating CMS Providers will continue to innovate in order to provide their subscribers with the best emergency alerting service it is feasible for them to offer. In this regard, we clarify that the geo-targeting requirement we adopt today does not preclude Participating CMS Providers from leveraging the location-sensing capability of WEA-capable mobile devices on their networks to geo-target Alert Message more accurately. As discussed below, the Commission will be adopting even more granular, handset-based, geo-targeting requirements. Our ultimate objective is for all Participating CMS Providers to match the target area provided by an alert originator.

69. Some alert originators remain concerned that a "best approximates" standard will continue to result in over-alerting and subsequent consumer opt-out. NYCEM, for example,

warns that the "best approximates" approach is vague and risks weakening our current geo-targeting requirement. While we do not adopt specific parameters for what constitutes "best approximates," we expect Participating CMS Providers to take reasonable efforts to leverage existing technology to its fullest extent, as noted above. We observe that in a recently adopted report, CSRIC V articulates expectations for cell broadcast-based geo-targeting in rural, suburban and urban areas pursuant to a "best approximates" approach. Specifically, in rural areas, CSRIC V expects that Participating CMS Providers would be able to approximate the target area with 30,000 meters of "overshoot." In suburban areas, where cell broadcast facilities are likely to be more densely deployed, CSRIC V expects that geo-targeting would become more accurate, achieving an average overshoot of five miles. In urban areas, CSRIC V expects that geo-targeting would be more accurate still, averaging two miles of overshoot. We find that these values would satisfy reasonable efforts to "best approximate" the alert area, consistent with our requirement. In this regard, we believe we strike an appropriate balance between the limitations of Participating CMS Providers' current geo-targeting capabilities using cell broadcast, and WEA stakeholders' goal of sending WEA Alert Messages only to those members of the public who are at risk.

70. We find that compliance with this geo-targeting requirement is technically feasible, and, in fact, every commenting CMS Provider except one states that they already use network-based cell broadcast techniques, such as algorithm-based facility selection and cell sectorization, to geo-target Alert Messages to polygonal areas more granular than required by our current "county-level" requirement. In this sense, the rule we adopt today will require most Participating CMS Providers only to continue to employ the techniques that they have been deploying as a matter of best practice. Emergency managers such as the NWS have also already

transitioned from county- to polygon-level geo-targeting, and express a need for WEA to keep pace with their ability to forecast with granularity the areas that will be impacted by weather events. We observe that in the event Participating CMS Providers are unable to practice polygon-level geo-targeting, we continue to allow Participating CMS Providers to transmit Alert Messages to an area not exceeding the propagation area of a single transmission site, as described in Section 10.450. We make conforming amendments to Section 10.450, however, to reflect the new geo-targeting standard that we adopt today and specify that "[i]f, however, the Participating CMS Provider cannot broadcast the Alert Message to an area that best approximates the target area, a Participating CMS Provider may transmit the Alert Message to an area not larger than the propagation area of a single transmission site."

71. Participating CMS Providers' support for polygon-level geo-targeting will produce significant public safety benefits. Relative to county-level geo-targeting, we expect that polygon-level geo-targeting will reduce over-alerting. When the public regularly receives alerts that do not apply to them, it creates alert fatigue, a driving factor behind consumers' decisions to opt out of receiving WEA Alert Messages. Further, the Houston Office of Public Safety and Homeland Security comments that "[c]ounty-level WEA warning is not only inconvenient, but can be dangerous, as protective actions may vary depending on the proximity to the hazard." Under-alerting also poses severe public safety risks. According to Austin Homeland Security and Emergency Management, under a county-level geo-targeting standard, "if there are no cell towers physically located in the warning area, the alert may not be transmitted at all by some carriers." This would be impermissible under the "best approximates" standard we adopt today. We also agree with Dennis Mileti, Professor Emeritus of Sociology at The University of Colorado, that with improved geo-targeting, "it is quite likely that milling after a received WEA

message would decrease since people would not need to determine if they are in the intended audience for the WEA." A reduction in milling is desirable because it reduces the delay between the time an Alert Message is received, and the time that the public will begin to take protective action. This reduction in milling behavior is also likely to benefit Participating CMS Providers by reducing network usage at times when their network is otherwise vulnerable to congestion due to the pending emergency event. Finally, we agree with BRETSA and Douglas County Emergency Management that more granular alerting will encourage emergency managers to become authorized as WEA alert originators. Simply put, Participating CMS Providers' support for polygon-level geo-targeting is an important step towards ensuring that everyone affected by an emergency has access to the emergency information provided by WEA, and contributes to the public perception that "if you receive a WEA, take action, because it applies to you."

72. Our decision to require support for Participating CMS Providers' best approximation of the target area is an important step towards ensuring that WEA Alert Messages can be sent to only those individuals for whom they are relevant. The record shows that over-alerting leads to alert fatigue, residents that ignore the Alert Messages, and public safety officials who refrain from using WEA in emergencies. The record also demonstrates consensus among emergency managers and Participating CMS Providers that we should clear a path forward for even more accurate geo-targeting, and that we should make progress towards the achievement of this goal by adopting an appropriate regulatory framework, and by continuing to collaborate with WEA stakeholders to establish standards and best practices, and to better understand technical issues. Recognizing that standards development and network modifications may be necessary to further improve geo-targeting, in the Further Notice we seek comment on any issues that remain to be addressed and on an appropriate timeframe for compliance.

73. Finally, we take action to ensure that emergency alert originators better understand the manner in which their messages will be geo-targeted. In the WEA NPRM we sought comment on whether to require Participating CMS Providers to report data to alert originators about their provision of WEA along key performance metrics, including the accuracy of geo-targeting. In response, emergency managers observe that information about geo-targeting, in particular, would be helpful to inform their emergency response planning efforts by improving transparency and understanding of IPAWS/WEA among emergency managers authorized to use WEA. Commenters also indicate that this transparency, in turn, could increase WEA adoption by non-participating emergency managers. In light of the demonstrated benefits of improving emergency managers' understanding of the geographic area to which their WEA Alert Messages will be targeted, we require that, upon request from an emergency management agency, a Participating CMS Provider will disclose information regarding their capabilities for geo-targeting Alert Messages (e.g., whether they are using network-based technology to "best approximate" the target area, or whether they are using device-based geo-fencing). A Participating CMS Provider is only required to disclose this information to an emergency management agency insofar as it would pertain to Alert Messages initiated by that emergency management agency, and only so long as the emergency management agency offers confidentiality protection at least equal to that provided by the federal FOIA.

3. Presenting Alert Messages Concurrent with Other Device Activity

74. We amend Section 10.510 to require WEA-capable mobile devices to present WEA Alert Messages as soon as they are received. We expect that devices engaged in active voice or data sessions on 4G-LTE networks will receive and prominently present WEA Alert Messages as soon as they are available, whereas WEA-capable mobile devices engaged in active

voice or data sessions on legacy networks will not be able to receive available Alert Messages until the active voice or data session concludes. This approach is consistent with the ATIS/TIA Mobile Device Behavior Specification's treatment of Alert Message prioritization.

75. We also allow Participating CMS Providers to provide their subscribers with the option to specify how the vibration cadence and attention signal should be presented when a WEA Alert Message is received during an active voice or data session in a manner that does not "preempt" it. Pursuant to the ATIS/TIA Mobile Device Behavior Specification, a "momentary interruption of a voice call or active data session, such as a brief visual, audible and/or vibration indication that a CMAS message has been received, is not considered preemption so long as the voice call/data session is not terminated and facilities to support that voice call or data session are not seized or released." We note that, according to ATIS, WEA-capable mobile devices currently take a variety of approaches to the use of the vibration cadence and audio attention signal to make the user aware of the receipt of an Alert Message while he/she is engaged in other device activity, but, according to AT&T, it "is possible to display the WEA alert in LTE VoLTE with the alert tone suppressed" during active voice sessions. We encourage Participating CMS Providers to leverage this capability by providing their customers with the option to change the manner in which the common attention signal and vibration cadence are used during active voice and data sessions.

76. This approach reflects the critical importance of a WEA Alert Message to its recipient, while also respecting that the Alert Message recipient may be using their mobile device to engage in a protective action that should not be interrupted, such as placing a call to 911, at the time the Alert Message is received. This approach is consistent with mobile device manufacturers' perspective that giving full priority to WEA Alert Messages during active voice

calls "would be distracting to the user," and that the WEA Alert Message should not disrupt the voice telephony capability of the device. It is also consistent with emergency managers' perspective that the readily recognizable common attention signal and vibration cadence should be presented to the public as quickly as technically possible, particularly during emergency situations where every second is critical. Conversely, we agree with commenters that a "priority access" requirement that would require ongoing voice and data sessions to be terminated by the receipt of a WEA Alert Message would not be in the public interest because it could result in the termination of other critical emergency communications.

C. Testing and Outreach

1. Supporting State/Local WEA Testing and Proficiency Training Exercises

77. We require Participating CMS Providers to support State/Local WEA Tests, as proposed in the WEA NPRM. Specifically, we adopt a new Section 10.350(c) to require Participating CMS Providers to support the receipt of State/Local WEA Tests from the Federal Alert Gateway Administrator, and to distribute such tests to the desired test area in a manner consistent with the Commission's Alert Message requirements. We reason that requiring State/Local WEA Tests to be received and delivered in accordance with our Alert Message requirements will ensure that emergency managers have the opportunity to test in an environment that mirrors actual alert conditions and evaluate, for example, the accuracy with which various Participating CMS Providers geo-target Alert Messages in their community. Unlike other Alert Messages, however, consumers will not receive State/Local WEA Tests by default. Participating CMS Providers should provide their subscribers with the option to receive State/Local WEA Tests, and subscribers would have to affirmatively select this option in order to

receive these test messages. According to CTIA, "[t]his way, unwanted test messages will not disturb wireless consumers who could become confused or annoyed by test messages and opt out of WEA entirely." We also agree with Sprint that making State/Local WEA Tests available on an opt-in basis minimizes any risk of call center congestion. Another respect in which a State/Local WEA Test will differ from an actual Alert Message is that we require State/Local WEA Tests to include conspicuous language sufficient to make clear to the public that the message is, in fact, only a test. This will minimize any chance that such test messages might be misconstrued as actual Alert Messages.

78. The 24-hour delivery window that currently applies to RMTs under Section 10.350(a)(2) will not apply to State/Local WEA Tests. Rather, we require that Participating CMS Providers transmit State/Local WEA Tests immediately upon receipt. We agree with commenters that allowing Participating CMS Providers to delay delivery of State/Local WEA Tests would make it impossible for emergency managers to evaluate message delivery latency, and might result in individuals who do opt in to receive State/Local WEA Tests receiving them in the middle of the night, which is unlikely to promote participation. A Participating CMS Provider may not forgo or delay delivery of a State/Local WEA Test, except when the test is preempted by actual Alert Message traffic, or if an unforeseen condition in the Participating CMS Provider infrastructure precludes distribution of the State/Local WEA Test. If a Participating CMS Provider Gateway forgoes or delays a State/Local WEA Test for one of these reasons, it shall send a response code to the Federal Alert Gateway indicating the reason consistent with how we currently require Participating CMS Providers to handle forgone RMTs. We anticipate that allowing Participating CMS Providers to forgo transmittal of a State/Local WEA Test if it is preempted by actual alert traffic or if unforeseen conditions arise will ensure

that State/Local WEA Tests do not "overwhelm wireless provides' limited resources, " as stated by CTIA. We defer to emergency managers to determine how frequently testing is appropriate, given this constraint.

79. We encourage emergency management agencies to engage in proficiency training exercises using this State/Local WEA Testing framework where appropriate. We agree with commenters that proficiency training exercises are a helpful and meaningful way for emergency managers to engage with alert and warning issues. Moreover, we agree with San Joaquin County OES that "proficiency training is an essential element of verifying competency" in the alert origination skill set necessary to issue effective WEA Alert Messages. We observe that our rules allow such proficiency training exercises now. We agree with APCO that alert origination software can be used to support internal proficiency training exercises where emergency managers wish to iterate alert origination best practices in a closed environment, and that the State/Local WEA Testing framework described above is sufficient to support cases where emergency management agencies find it appropriate to involve the public in their WEA exercises. We hope that proficiency training exercises will provide emergency management agencies with a method of generating their own WEA alert origination best practices, particularly with respect to the kinds of enhanced Alert Messages enabled by this proceeding (i.e., Alert Messages up to 360 characters in length that may include embedded references, may be issued in Spanish, and may be intended to supplement an already-issued Alert Message).

80. We find that requiring Participating CMS Providers to support this State/Local WEA Testing framework is technically feasible, requiring only updates to software and standards in order to allow users the option to opt in to receive such tests, and that it will result in significant public safety benefits. Specifically, we agree with Clarion County OES and the

Lexington Division of Emergency Management that while occasional system failures are probable, a solid testing and training platform such as this can ensure that failures can be corrected during a period where no real emergency exists. We also agree with Calcasieu Parish Police Jury Office of Homeland Security and Emergency Preparedness that regular readiness testing and proficiency training are critical to maintaining WEA alert origination competency because "[i]f you don't use it you lose it." According to FEMA, requiring Participating CMS Providers to support State/Local WEA Testing will improve WEA by providing confidence to the public that their handsets are capable of receiving an Alert Message from local emergency management agencies, and by rendering WEA suitable for use in coordinated public warning exercises, such as those required by the Nuclear Regulatory Commission for local emergency preparedness programs. Further, we agree with Harris County Office of Homeland Security and Emergency Management that State/Local WEA Tests, in conjunction with targeted outreach efforts, may be useful to emergency managers as a tool to improve their competency at initiating Alert Messages in languages other than English. Importantly, emergency managers may also use State/Local WEA Tests to voluntarily collect and share information about geo-targeting, alert delivery latency, and other vital performance metrics. We encourage emergency managers and related entities to engage in extensive outreach to their respective communities in order to socialize the benefits of public participation in State/Local WEA Tests, and otherwise to raise public awareness about the benefits of receiving WEA messages, including through the use of PSAs.

2. Testing the NCE Public Television C-interface Back-up

81. We agree with the public broadcasting and NCE commenters that in order to be fully effective and reflective of WEA system needs, a test of the public television broadcast-

based backup to the C-interface should be implemented as an end-to-end test from the IPAWS to the CMS Provider Gateways. Accordingly, we amend our rules to make it clear that periodic C interface testing must include the testing of its public television broadcast-based backup. Pursuant to this framework, FEMA would initiate a test of the broadcast-based C-interface backup by sending a test message through that infrastructure to the CMS Provider Alert Gateway, which would respond by returning an acknowledgement of receipt of the test message to the FEMA Gateway. This approach ensures reliable continuity between FEMA and Participating CMS Providers, even during a disaster in which internet connectivity may be lost. We defer to FEMA as the IPAWS and Federal Alert Gateway administrator to determine the periodicity of these tests in conversation with Participating CMS Providers.

82. By requiring CMS Providers to participate in periodic testing of the broadcast-based backup to the C-interface, "we develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services," as recommended by the CSRIC V WEA Security Report. PBS, APTS, and CPB agree that this approach to testing the C-interface backup presents NCE public broadcasting entities with no additional cost burdens. We agree with PBS, APTS, and CPB that this rule will require no "material intervention" by such stations because their receipt and retransmission of test messages will be entirely automated, and will use equipment already installed at their facilities. Accordingly, we anticipate that stations in compliance with our rules today will have to take no additional steps in order to comply with this new testing requirement.

3. Facilitating WEA PSAs

83. We amend Sections 11.45 and 10.520 to allow federal, state and local, tribal and territorial entities, as well as non-governmental organizations (NGOs) in coordination with such

entities, to use the attention signal common to EAS and WEA to raise public awareness about WEA. WEA PSAs that use the WEA attention signal must make clear that it is being used in the context of the PSA, "and for the purpose of educating the viewing or listening public about the functions of their WEA-capable mobile devices and the WEA program," including by explicitly stating that the WEA attention signal is being used in the context of a PSA for the purpose of educating the public about WEA.

84. We agree with commenters that facilitating federal, state, local, tribal and territorial governments' issuance of WEA PSAs, as proposed, is in the public interest, and that the utility of WEA PSAs will only be augmented by allowing NGOs to produce them in coordination with governmental entities by promoting effective community partnership. Specifically, WEA PSAs can be effective tools to raise public awareness about, and promote positive perceptions of WEA, which may reduce consumer opt-out and reduce milling. We note the PSA campaign of Minnesota Emergency, Community Health and Outreach (ECHO), a program and service of Twin Cities Public Television, as an example of how governmental entities can partner with NGOs to raise community awareness about the significance of the common alerting attention signal for EAS and WEA. We also note that WEA PSAs have become a critical part of FEMA's Ready campaign that has "shown that it can enhance the public's understanding of how the WEA functions and increase the public's benefits from the WEA and thereby benefit public safety generally." We agree with commenters that the issuance of WEA PSAs is particularly appropriate in the context of the rules we adopt today. For example, with respect to increasing the maximum WEA character limit, FEMA notes that it will "need to . . . conduct additional public information efforts to inform people of the new format of Alert Messages they may receive on their cellular phones." Additionally, we anticipate that

PSAs will be an effective method to acclimate the public to the fact that they may receive supplemental instructions about how to respond to an emergency through the newly adopted WEA Public Safety Message classification. Indeed, we commit to work with WEA stakeholders to develop community outreach plans and raise public awareness about each of the WEA enhancements made possible by this Report and Order. Moreover, we agree with Professor Denis Mileti, Professor Emeritus, University of Colorado, that WEA PSAs can reduce milling by "build[ing] the reputation of the WEA system with the American public," making it a more credible and authoritative single resource for emergency information.

D. Compliance Timeframes

RULE AMENDMENT	COMPLIANCE TIMEFRAME	RULE(S) AFFECTED
Increasing Maximum WEA Character Length	Within 30 months of the rule's publication in the Federal Register	47 CFR 10.430
Classifying Public Safety Messages	Within 30 months of the rules' publication in the Federal Register	47 CFR 10.280(a) 47 CFR 10.400(d) 47 CFR 10.410
Supporting Embedded References and Multimedia	The removal of our prohibition on the use of embedded references is effective 30 days from the rules' publication in the Federal Register. Our requirement to support	47 CFR 10.440 47 CFR 10.441

RULE AMENDMENT	COMPLIANCE TIMEFRAME	RULE(S) AFFECTED
	embedded references is effective one year from the rules' publication in the Federal Register.	
Spanish-language Alerting	Within 2 years of the rule's publication in the Federal Register	47 CFR 10.480
Alert Logging	Within 60 days of publication in the Federal Register of a notice announcing the approval by the Office of Management and Budget of the modified information collection requirements	47 CFR 10.320(g)
WEA Geo-targeting	Within 60 days of the rule's publication in the Federal Register	47 CFR 10.450
WEA Presentation	Within 30 months of the rule's publication in the Federal Register	47 CFR 10.510

RULE AMENDMENT	COMPLIANCE TIMEFRAME	RULE(S) AFFECTED
State/Local WEA Testing	Within 30 months of the rule's publication in the Federal Register	47 CFR 10.350(c)
C-interface Backup Testing	Within 30 days of the rule's publication in the Federal Register	47 CFR 10.350(b)
WEA PSAs	Within 30 days of the rule's publication in the Federal Register	47 CFR 10.520(d)

85. Therefore, nationwide Participating CMS Providers' subscribers should have greater confidence that WEA Alert Messages they receive are intended for them as of February, 2017. Participating CMS Providers' subscribers should expect to be able to receive Alert Messages in Spanish by 2019. Then, by June 2019, they should expect to see 360-character maximum alerts on 4G LTE and future networks, Public Safety Messages, Alert Messages that contain embedded references, and State/Local WEA Tests presented as soon as they are received. While we expect that updates to our WEA PSA, C-interface backup testing, and alert logging rules will produce significant public safety benefits, as described below, we do not anticipate that consumers will immediately notice a change in service due to these updates.

II. ORDERING CLAUSES

86. Accordingly, IT IS ORDERED, pursuant to sections 1, 2, 4(i), 4(o), 301, 303(r),

303(v), 307, 309, 335, 403, 624(g), 706, and 715 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 152, 154(i), 154(o), 301, 301(r), 303(v), 307, 309, 335, 403, 544(g), 606, and 615, as well as by sections 602(a),(b),(c), (f), 603, 604 and 606 of the WARN Act, 47 U.S.C. 1202(a),(b),(c), (f), 1203, 1204 and 1206, that the WEA Report and Order and Further Notice of Proposed Rulemaking in PS Docket Nos. 15-91 and 15-94 IS HEREBY ADOPTED.

87. IT IS FURTHER ORDERED that the Commission's rules ARE HEREBY AMENDED as set forth in Appendix A.

88. IT IS FURTHER ORDERED that the rules adopted herein WILL BECOME EFFECTIVE as described herein,[1] including those rules and requirements which contain new or modified information collection requirements that require approval by the Office of Management and Budget (OMB) under the Paperwork Reduction Act that WILL BECOME EFFECTIVE after publication in the Federal Register of a notice announcing such approval and the relevant effective date.[2]

89. Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of the WEA Report and Order and Further Notice of Proposed Rulemaking, including the Final and Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

The rules in this part are issued pursuant to the authority contained in the Warning, Alert, and Response Network Act, Title VI of the Security and Accountability for Every Port Act of 2006, Pub. L. 109-347, Titles I through III of the Communications Act of 1934, as amended, and Executive Order 13407 of June 26, 2006, Public Alert and Warning System, 71 FR 36975 (June

[1] See supra Section 0 (D. Compliance Timeframes).

[2] Pub. L. 104-13, 109 Stat. 163 (May 22, 1995), codified at 44 USC 3501 et seq.

28, 2006).

List of Subjects

47 CFR Part 10

Communications common carriers, Emergency alerting.

47 CFR Part 11

Radio, Television, Emergency alerting.

FEDERAL COMMUNICATIONS COMMISSION.

Gloria J. Miles**,**
Federal Register Liaison Officer.
Office of the Secretary.

Final Rules

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR parts 10 and 11 to read as follows:

PART 10 – WIRELESS EMERGENCY ALERTS

1. The authority citation for part 10 continues to read as follows:

Authority: 47 U.S.C. 151, 154(i) and (o), 201, 303(r), 403, and 606; sections 602(a), (b), (c), (f), 603, 604 and 606 of Pub. L. 109-347, 120 Stat. 1884.

2. Effective May 1, 2019, § 10.280 is amended by revising paragraph (a) to read as follows:

§ 10.280 Subscribers' right to opt out of WEA notifications.

(a) CMS providers may provide their subscribers with the option to opt out of the "Child Abduction Emergency/AMBER Alert," "Imminent Threat Alert" and "Public Safety Message" classes of Alert Messages.

* * * * *

3. Effective on the date to be announced by the Commission in a document published in the Federal Register, § 10.320 is amended by adding paragraph (g) to read as follows:

§ 10.320 Provider alert gateway requirements.

* * * * *

(g) Alert logging. The CMS provider gateway must perform the following functions:

(1) Logging requirements. Log the CMAC attributes of all Alert Messages received at the CMS Provider Alert Gateway, including time stamps that verify when the message is received, and when it is retransmitted or rejected by the Participating CMS Provider Alert Gateway. If an Alert Message is rejected, a Participating CMS Provider is required to log the specific error code generated by the rejection.

(2) Maintenance of logs. Participating CMS Providers are required to maintain a log of all active and cancelled Alert Messages for at least 12 months after receipt of such alert or cancellation.

(3) Availability of logs. Participating CMS Providers are required to make their alert logs available to the Commission and FEMA upon request. Participating CMS Providers are also required to make alert logs available to emergency management agencies that offer confidentiality protection at least equal to that provided by the federal Freedom of Information Act (FOIA) upon request, but only insofar as those logs pertain to Alert Messages initiated by that emergency management agency.

4. Effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], § 10.350 is amended by revising the section heading, introductory text, and paragraph (b) to read as follows:

§ 10.350 WEA testing and proficiency training requirements.

This section specifies the testing that is required of Participating CMS Providers.

* * * * *

(b) Periodic C interface testing. In addition to the required monthly tests, a Participating CMS Provider must participate in periodic testing of the interface**s** between the Federal Alert Gateway and its CMS Provider Gateway, including the public television broadcast-based backup to the C-interface. This periodic interface testing is not intended to test the CMS Provider's infrastructure nor the mobile devices but rather is required to ensure the availability/viability of both gateway functions. Each CMS Provider Gateway shall send an acknowledgement to the Federal Alert Gateway upon receipt of such interface test messages. Real event codes or Alert Messages shall not be used for this periodic interface testing.

* * * * *

5. Effective May 1, 2019, § 10.350 is amended by adding paragraph (c) to read as follows:

§ 10.350 WEA testing and proficiency training requirements.

* * * * *

(c) State/Local WEA Testing. A Participating CMS Provider must support State/Local WEA Tests in a manner that complies with the Alert Message Requirements specified in Subpart D.

(1) A Participating CMS Provider's Gateway shall support the ability to receive a State/Local WEA Test message initiated by the Federal Alert Gateway Administrator.

(2) A Participating CMS Provider shall immediately transmit a State/Local WEA Test to the geographic area specified by the alert originator.

(3) A Participating CMS Provider may forego a State/Local WEA Test if the State/Local WEA Test is pre-empted by actual alert traffic or if an unforeseen condition in the CMS Provider infrastructure precludes distribution of the State/Local WEA Test. If a Participating CMS Provider Gateway forgoes a State/Local WEA Test, it shall send a response code to the Federal Alert Gateway indicating the reason.

(4) Participating CMS Providers shall provide their subscribers with the option to opt in to receive State/Local WEA Tests.

6. Effective May 1, 2019, § 10.400 is amended by revising the introductory text and adding paragraph (d) to read as follows:

§ 10.400 Classification.

A Participating CMS Provider is required to receive and transmit four classes of Alert Messages: Presidential Alert; Imminent Threat Alert; Child Abduction Emergency/AMBER Alert; and Public Safety Message.

* * * * *

(d) Public Safety Message. A Public Safety Message is an essential public safety advisory that prescribes one or more actions likely to save lives and/or safeguard property during an emergency. A Public Safety Message may only be issued in connection with an Alert Message classified in paragraphs (a), (b) or (c) of this section.

7. Effective May 1, 2019, § 10.410 is revised to read as follows:

§ 10.410 Prioritization.

A Participating CMS Provider is required to transmit Presidential Alerts upon receipt. Presidential Alerts preempt all other Alert Messages. A Participating CMS Provider is required to transmit Imminent Threat Alerts, AMBER Alerts and Public Safety Messages on a first in-first out (FIFO) basis.

8. Effective May 1, 2019, § 10.430 is revised to read as follows:

§ 10.430 Character limit.

A Participating CMS Provider must support transmission of an Alert Message that contains a maximum of 360 characters of alphanumeric text. If, however, some or all of a Participating CMS Provider's network infrastructure is technically incapable of supporting the transmission of a 360-character maximum Alert Message, then that Participating CMS Provider must support transmission of an Alert Message that contains a maximum of 90 characters of alphanumeric text on and only on those elements of its network incapable of supporting a 360 character Alert Message.

§ 10.440 [Removed].

9. Effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], remove § 10.440.

10. Effective November 1, 2017, § 10.441 is added to read as follows:

§ 10.441 Embedded references.

Participating CMS Providers are required to support Alert Messages that include an embedded Uniform Resource Locator (URL), which is a reference (an address) to a resource on the Internet, or an embedded telephone number.

11. Effective [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], § 10.450 is revised to read as follows:

§ 10.450 Geographic targeting.

This section establishes minimum requirements for the geographic targeting of Alert Messages.

(a) A Participating CMS Provider will determine which of its network facilities, elements, and locations will be used to geographically target Alert Messages. A Participating CMS Provider must transmit any Alert Message that is specified by a geocode, circle, or polygon to an area that best approximates the specified geocode, circle, or polygon. If, however, the Participating CMS Provider cannot broadcast the Alert Message to an area that best approximates the specified geocode, circle, or polygon, a Participating CMS Provider may transmit an Alert Message to an area not larger than the propagation area of a single transmission site.

(b) Upon request from an emergency management agency, a Participating CMS Provider will disclose information regarding their capabilities for geo-targeting Alert Messages. A Participating CMS Provider is only required to disclose this information to an emergency management agency insofar as it would pertain to Alert Messages initiated by that emergency management agency, and only so long as the emergency management agency offers confidentiality protection at least equal to that provided by the federal FOIA.

12. Effective November 1, 2018, § 10.480 is added to subpart D to read as follows:

§ 10.480 Language support.

Participating CMS Providers are required to transmit WEA Alert Messages that are issued in the Spanish language or that contain Spanish-language characters.

13. Effective May 1, 2019, § 10.510 is revised to read as follows:

§ 10.510 Call preemption prohibition.

Devices marketed for public use under part 10 must present an Alert Message as soon as they receive it, but may not enable an Alert Message to preempt an active voice or data session. If a mobile device receives a WEA Alert Message during an active voice or data session, the user may be given the option to control how the Alert Message is presented on the mobile device with respect to the use of the common vibration cadence and audio attention signal.

14. Effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], § 10.520 is amended by revising paragraph (d) to read as follows:

§ 10.520 Common audio attention signal.

*** * * * ***

(d) No person may transmit or cause to transmit the WEA common audio attention signal, or a recording or simulation thereof, in any circumstance other than in an actual National, State or Local Area emergency or authorized test, except as designed and used for Public Service Announcements (PSAs) by federal, state, local, tribal and territorial entities, and non-governmental organizations in coordination with those entities, to raise public awareness about emergency alerting, provided that the entity presents the PSA in a non-misleading manner, including by explicitly stating that the emergency alerting attention signal is being used in the context of a PSA for the purpose of educating the viewing or listening public about emergency alerting.

*** * * * ***

PART 11 – EMERGENCY ALERT SYSTEM

15. The authority citation for part 11 continues to read as follows:

Authority: 47 U.S.C. 151, 154 (i) and (o), 303(r), 544(g) and 606.

16. Effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], § 11.45 is revised to read as follows:

§ 11.45 Prohibition of false or deceptive EAS transmissions.

No person may transmit or cause to transmit the EAS codes or Attention Signal, or a recording or simulation thereof, in any circumstance other than in an actual National, State or Local Area emergency or authorized test of the EAS, or as specified in § 10.520(d) of this chapter.

[FR Doc. 2016-26120 Filed: 10/31/2016 8:45 am; Publication Date: 11/1/2016]