

DOCKET FILE COPY ORIGINAL

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

In the Matter of)
)
The Commercial Mobile Alert System)
)
)
)

PS Docket No. 07-287

MAILED
APR 16 2008
FCC

FIRST REPORT AND ORDER

Adopted: April 9, 2008

Released: April 9, 2008

By the Commission: Chairman Martin, and Commissioners Copps, Adelstein, Tate and McDowell issuing separate statements.

TABLE OF CONTENTS

Heading	Paragraph #
I. INTRODUCTION.....	1
II. BACKGROUND.....	5
III. DISCUSSION.....	7
A. Consideration of the CMSAAC Recommendations.....	8
B. CMAS Architecture and CMS Provider Functions.....	10
C. General CMAS Requirements.....	25
1. Scope and Definition of CMAS Alerts.....	26
a. Presidential Alerts.....	28
b. Imminent Threat Alerts.....	29
c. Child Abduction Emergency/AMBER Alerts.....	31
2. Technologically Neutral Alert System.....	33
3. CMAS Message Elements and Capabilities.....	41
a. Required Alert Message Elements.....	41
b. CMAS Generation of Free Text Alert Messages.....	44
4. Geo-targeting CMAS Alerts.....	48
5. Meeting the Needs of Users, Including Individuals with Disabilities and the Elderly.....	57
6. Output Mode/Display.....	68
7. Message Retransmission.....	70
8. Multi-Language CMAS Alerting.....	71
9. Roaming.....	78
10. Preemption of Calls in Progress.....	80
D. Service Profiles.....	81
E. Security for CMAS Alerts.....	87
F. CMAS Reliability and Performance.....	90
G. Timeline for Implementation of Technical Requirements, Standards and Protocols.....	92
IV. PROCEDURAL MATTERS.....	96
A. Final Regulatory Flexibility Act Analysis.....	96
B. Final Paperwork Reduction Act of 1995 Analysis.....	97

C. Congressional Review Act Analysis.....	98
D. Alternative Formats.....	99
V. ORDERING CLAUSES.....	100
APPENDIX A - List Of Commenters	
APPENDIX B - Final Regulatory Flexibility Analysis	
APPENDIX C - Final Rules.....	

I. INTRODUCTION

1. This Commercial Mobile Alert System First Report and Order (CMAS First Report and Order) represents our next step in establishing a Commercial Mobile Alert System (CMAS), under which Commercial Mobile Service (CMS) providers¹ may elect to transmit emergency alerts to the public. We take this step in compliance with section 602(a) of the WARN Act,² which requires the Commission to adopt “relevant technical standards, protocols, procedures, and other technical requirements” based on the recommendations of the Commercial Mobile Service Alert Advisory Committee (CMSAAC) “necessary to enable commercial mobile service alerting capability for commercial mobile service providers that voluntarily elect to transmit emergency alerts.”

2. In this CMAS First Report and Order, we adopt rules necessary to enable CMS alerting capability for CMS providers who elect to transmit emergency alerts to their subscribers. Specifically, we adopt the architecture for the CMAS proposed by the CMSAAC and conclude that a Federal Government entity should aggregate, authenticate, and transmit alerts to the CMS providers. In addition, we adopt technologically neutral rules governing:

- *CMS provider-controlled elements within the CMAS architecture* (e.g., the CMS Provider Gateway, CMS Provider infrastructure and mobile devices);
- *Emergency alert formatting, classes, and elements*: Participating CMS Providers must transmit three classes of alerts - Presidential, Imminent Threat, and AMBER alerts;
- *Geographic targeting (geo-targeting)*: Participating CMS Providers generally are required to target alerts at the county-level as recommended by the CMSAAC;
- *Accessibility for people with disabilities and the elderly*: Participating CMS Providers must include an audio attention signal and vibration cadence on CMAS-capable handsets;
- *Multi-language Alerting*: Participating CMS Providers will not be required at this time to transmit alerts in languages other than English;
- *Availability of CMAS alerts while roaming*: Subscribers receiving services pursuant to a roaming agreement will receive alert messages on the roamed upon network if the operator of the roamed upon network is a Participating CMS provider and the subscriber's mobile device is configured for and technically capable of receiving alert messages from the roamed upon network;

¹ For purposes of section 602 of the Warning, Alert and Response Network (WARN) Act, Congress specifically defined “commercial mobile service” as that found in section 332(d)(1) of the Communications Act of 1934, as amended, 47 U.S.C. § 332(d)(1) (the term “commercial mobile service” means any mobile service that is provided for profit and makes interconnected service available to the public or to such classes of eligible users as to be effectively available to a substantial portion of the public, as specified by regulation by the Commission). Warning, Alert, and Response Network Act, Title VI of the Security and Accountability for Every Port Act of 2006, Pub. L. No. 109-347, 120 Stat. 1884, (2006), 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 Fed. Reg. 36975 (June 26, 2006) (WARN Act), § 602(b)(1)(A) (*Executive Order 13407*).

² WARN Act, § 602(a).

- *Preemption of calls in progress:* CMAS alerts may not preempt a voice or data session in progress;
- *Initial implementation:* Participating CMS Providers must comply with these rules no later than 10 months from the date the FCC announces the selection of a Federal Government entity to perform the Alert Aggregator and Alert Gateway functions required to implement the CMAS.

3. In adopting these rules today, we take a significant step towards implementing one of our highest priorities – to ensure that all Americans have the capability to receive timely and accurate alerts, warnings and critical information regarding disasters and other emergencies irrespective of what communications technologies they use. As we have learned from disasters such as the 2005 hurricanes, such a capability is essential to enable Americans to take appropriate action to protect their families and themselves from loss of life or serious injury. This CMAS First Report and Order also is consistent with our obligation under Executive Order 13407³ to “adopt rules to ensure that communications systems have the capacity to transmit alerts and warnings to the public as part of the public alert and warning system,”⁴ and our mandate under the Communications Act to promote the safety of life and property through the use of wire and radio communication.⁵

4. This CMAS First Report and Order is the latest step of our ongoing drive to enhance the reliability, resiliency, and security of emergency alerts to the public by requiring that alerts be distributed over diverse communications platforms. In the 2005 EAS First Report and Order, we expanded the scope of the Emergency Alert System (EAS) from analog television and radio to include participation by digital television broadcasters, digital cable television providers, digital broadcast radio, Digital Audio Radio Service (DARS), and Direct Broadcast Satellite (DBS) systems.⁶ As we noted in the Further Notice of Proposed Rulemaking that accompanied the EAS First Report and Order, wireless services are becoming equal to television and radio as an avenue to reach the American public quickly and efficiently.⁷ As of June 2007, approximately 243 million Americans subscribed to wireless services.⁸ Wireless service has progressed beyond voice communications and now provides subscribers with access to a wide range of information critical to their personal and business affairs. In times of emergency, Americans increasingly rely on wireless telecommunications services and devices to receive and retrieve critical, time-sensitive information. A comprehensive wireless mobile alerting system would have the ability to alert people on the go in a short timeframe, even where they do not have access to broadcast radio or television or other sources of emergency information. Providing critical alert information via wireless devices will ultimately help the public avoid danger or respond more quickly in the face of crisis, and thereby save lives and property.

³ Public Alert and Warning System, Exec. Order No. 13407, 71 Fed. Reg. 36975 (Jun. 26, 2006) (*Executive Order 13407*). In Executive Order 13407, the President noted that it was the “policy of the United States to have an effective, reliable, integrated, flexible, and comprehensive system to alert and warn the American people in situations of war, terrorist attack, natural disaster, or other hazards to public safety and well-being . . .,” and established certain obligations in this regard for the Department of Homeland Security, the National Oceanic & Atmospheric Administration (NOAA), and the FCC.

⁴ *Executive Order 13407*, § 3(b)(iii).

⁵ See 47 U.S.C. § 151.

⁶ See, e.g., Review of the Emergency Alert System, EB Docket No. 04-296, *First Report and Order*, 20 FCC Rcd 18625 (2005) (EAS First Report and Order and Further Notice)

⁷ *Id.* at 18625, 18653.

⁸ Cellular Telecommunications & Internet Association, Mid-Year 2007 Top-Line Survey Results, available at http://files.ctia.org/pdf/CTIA_Survey_Mid_Year_2007.pdf (last visited on Mar. 18, 2008).

II. BACKGROUND

5. On October 13, 2006, the President signed the Security and Accountability For Every Port (SAFE Port) Act into law.⁹ Title VI of the SAFE Port Act, the Warning Alert and Response Network (WARN) Act, establishes a process for the creation of the CMAS whereby CMS providers may elect to transmit emergency alerts to their subscribers. The WARN Act requires that we undertake a series of actions to accomplish that goal, including requiring the Commission, by December 12, 2006 (within 60 days of enactment), to establish and convene an advisory committee to recommend system critical protocols and technical capabilities for the CMAS.¹⁰ Accordingly, we formed the CMSAAC, which had its first meeting on December 12, 2006.¹¹ The WARN Act further required the CMSAAC to submit its recommendations to the Commission by October 12, 2007 (one year after enactment).¹² The CMSAAC submitted its report to us on that date.¹³

6. Section 602(a) of the WARN Act further requires that, by April 9, 2008 (within 180 days of receipt of the CMSAAC's recommendations), the Commission complete a proceeding to adopt "relevant technical standards, protocols, procedures and technical requirements" based on recommendations submitted by the CMSAAC, "necessary to enable commercial mobile service alerting capability for commercial mobile service providers that voluntarily elect to transmit emergency alerts."¹⁴ On December 14, 2007, we released the Notice of Proposed Rulemaking¹⁵ requesting comment on, among other things, the technical requirements we should adopt to facilitate CMS providers' voluntary transmission of emergency alerts.¹⁶ We specifically invited comment on the CMSAAC's proposed technical requirements. Comments were due on February 4, 2008, with Reply Comments due on February 19, 2008.¹⁷

⁹ See *supra*, n.1.

¹⁰ WARN Act, § 603(a), (d).

¹¹ As required by the WARN Act, the CMSAAC consisted of representatives from state and local governments, federally recognized Indian tribes, representatives of the communications industry, including both wireless service providers and broadcasters, vendors and manufacturers and national organizations representing people with special needs. The Committee also included other qualified stakeholders such as representatives of the Federal Emergency Management Agency (FEMA) and NOAA. See Notice of Appointment of Members to the Commercial Mobile Service Alert Advisory Committee; Agenda for December 12, 2006 Meeting, *Public Notice*, 21FCC Rcd 14175 (PSHSB 2006).

¹² WARN Act, § 603(c).

¹³ The CMSAAC held six meetings during which it received progress reports from its internal working groups and presentations from interested parties. On October 3, 2007, the Committee approved a set of recommendations and submitted them on October 12, 2007. In developing its recommendations, the CMSAAC consulted the National Institute of Standards and Technology (NIST), as required by section 603(g) of the WARN Act.

¹⁴ WARN Act, § 602(a).

¹⁵ The Commercial Mobile Alert System, PS Docket No. 07-287, *Notice of Proposed Rulemaking*, 22 FCC Rcd 21975 (2007) (*CMAS NPRM*).

¹⁶ In the *CMAS NPRM*, we also sought comment on issues related to other provisions of the WARN Act such as section 602(b) (requiring, among other things, that the Commission establish a mechanism for CMS providers to elect to participate in CMAS); section 602(c) (requiring the Commission to require noncommercial educational (NCE) broadcasters to install equipment to support geographically targeted (geo-targeting) alerts by CMS providers) and section 602(f) (authorizing the Commission to require testing of the CMAS). We will address these provisions of the WARN Act and related issues in subsequent Orders within the deadlines established by the statute. See *CMAS NPRM*, 22 FCC Rcd at 21976-21978, ¶ 5.

¹⁷ A list of the parties commenting on the *CMAS NPRM* is attached at Appendix A.

III. DISCUSSION

7. Consistent with section 602(a) of the WARN Act, today we adopt ‘technical standards, protocols, procedures and other technical requirements . . . necessary to enable commercial mobile service alerting capability for commercial mobile service providers that voluntarily elect to transmit emergency alerts.’¹⁸ Specifically, the rules we adopt today address the CMS providers’ functions within the CMAS, including CMS provider-controlled elements within the CMAS architecture, emergency alert formatting, classes and elements, geographic targeting (geo-targeting) and accessibility for people with disabilities and the elderly.¹⁹ In most cases, we have adopted rules generally based on the CMSAAC recommendations.²⁰ In such cases, we find that the CMSAAC’s recommendations are supported by the record and that adoption of those recommendations serves the public interest and meets the requirements of the WARN Act. For reasons discussed below, however, in some cases, we have determined that the public interest requires us to adopt requirements that are slightly different than those recommended by the CMSAAC.

A. Consideration of the CMSAAC Recommendations

8. Several entities representing the wireless industry generally argue in their comments that the Commission has no authority to adopt technical requirements other than those proposed by the CMSAAC and that those must be adopted “as is.”²¹ We disagree. The WARN Act does not require that we adopt the CMSAAC’s recommendations verbatim. Rather, Congress required the Commission to adopt relevant technical requirements “based on recommendations of the CMSAAC.”²² This indicates that while Congress intended that we give appropriate weight to the CMSAAC’s recommendations in our adoption of rules, it did not intend to require the Commission to adopt the CMSAAC’s recommendations wholesale, without any consideration for views expressed by other stakeholders in the proceeding or the need to address other significant policy goals.²³ Moreover, adopting the CMSAAC’s recommendations in their entirety, without scrutiny, would result in an abdication of the Commission’s statutory mandate under the Communications Act to act in the public interest. Clearly the WARN Act did not delegate Commission authority under the Communications Act to an advisory committee; on the contrary, the Commission was to conclude a “proceeding” which necessarily implicates notice and an opportunity for public comment, and Commission discretion in adopting appropriate rules and requirements.

9. Commission discretion and flexibility in its adoption of the CMSAAC recommendations is also supported by the policy goal underlying the WARN Act, *i.e.*, the creation of a CMAS in which CMS providers will elect to participate, and which will effectively deliver alerts and warnings to the public. The comments of Ericsson, with which we agree, support Commission discretion by stating that the technical standards and requirements we adopt for the CMAS should account for an evolving

¹⁸ WARN Act, § 602(a).

¹⁹ As required by section 602(a) of the WARN Act, we consulted the NIST in our adoption of technical rules.

²⁰ We note that the overwhelming majority of commenters support our adoption of the CMSAAC recommendations. *See, e.g.*, T-Mobile Comments at 2, 3G America Comments at 11, CTIA Comments at 19, TIA Comments at 10, AT&T Comments at 20, Ericsson, Inc. (Ericsson) Comments at 6, Rural Cellular Association Comments at 1-2.

²¹ *See, e.g.*, Verizon Wireless Comments at 6, Verizon Wireless Reply Comments at 2-3, Rural Cellular Association (RCA) Comments at 2-4, Alltel Comments at 2.

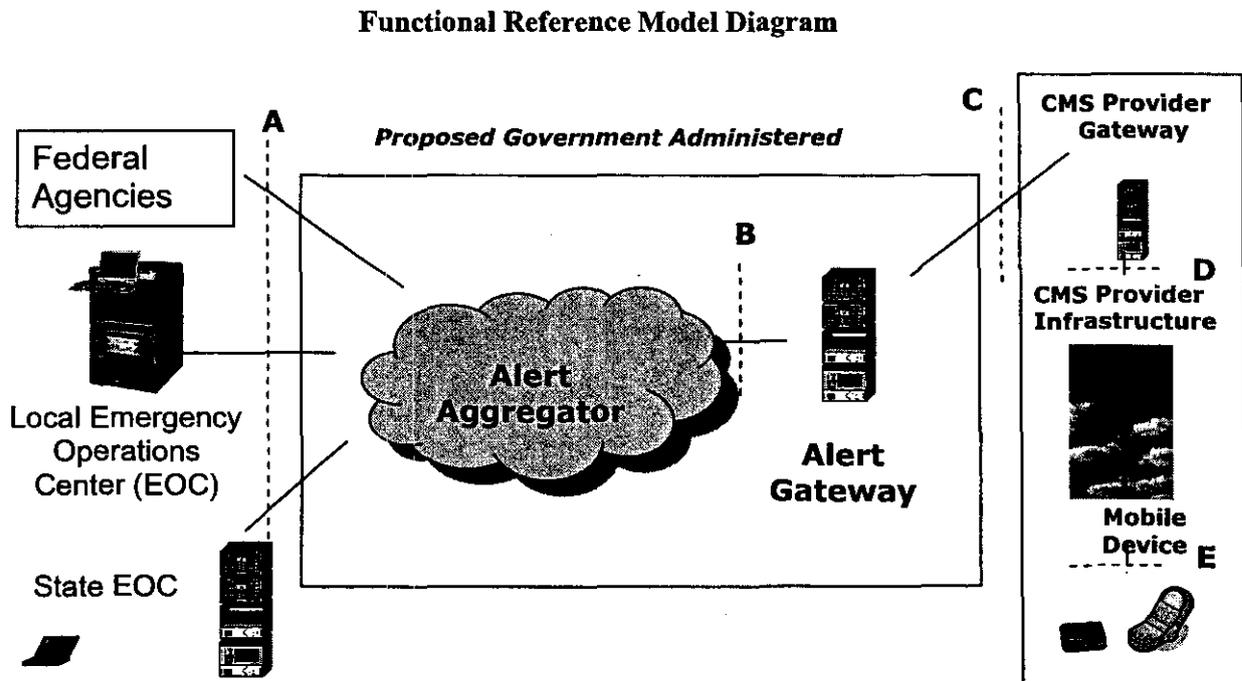
²² *See* WARN Act, § 602(a).

²³ Had Congress, as some commenters suggest, intended to require that the Commission adopt the CMSAAC’s recommendations “as is,” Congress would have simply said so. Moreover, the commenters’ reading of the statute appears inconsistent with Congress’ direction that both the CMSAAC and the Commission, separately, consult NIST. *Cf.* WARN Act § 602(a) and § 603(g). There would have been no need for the Commission to consult NIST again if, as the commenters suggest, Congress intended the Commission to simply adopt the CMSAAC’s recommendations “as is.”

technology landscape.²⁴ In order to account for changes in the wireless industry and maintain a technologically neutral approach to emergency alerting, the Commission must be able to apply the CMSAAC's recommendations to new technologies and services. A reasonable interpretation of the WARN Act, therefore, is that the Commission has the discretion to evaluate the CMAS technical requirements recommended by the CMSAAC.

B. CMAS Architecture and CMS Provider Functions

10. In its recommendations, the CMSAAC proposed the following architecture for the CMAS.²⁵



Under this proposed reference model, a Federal government entity, the "Alert Aggregator," operating under a "Trust Model,"²⁶ would receive, aggregate, and authenticate alerts originated by authorized alert initiators (*i.e.*, Federal, state, tribal and local government agencies) using the Common Alerting Protocol (CAP).²⁷ The Federal government entity would also act as an "Alert Gateway"²⁸ that would formulate a 90 character alert based on key fields in the CAP alert sent by the alert initiator.²⁹ Based on CMS provider profiles maintained in the Alert Gateway, the Alert Gateway would then deliver the alert over a

²⁴ Ericsson Comments at 5.

²⁵ See CMSAAC recommendations, § 2.1, figure2-1 (CMAS Functional Reference Model).

²⁶ See CMSAAC recommendations, § 8.

²⁷ The Common Alerting Protocol (CAP) refers to Organization for the Advancement of Structured Information Standards (OASIS) Standard CAP-V1.1, October 2005.

²⁸ See CMSAAC recommendations, § 2.2.4

²⁹ Provisions have also been made for authorized alert originators to formulate and distribute alerts via the Alert Gateway in free text. See *e.g.*, CMSAAC recommendations, § 5.3.2.

secure interface operated by the CMS provider³⁰ to another gateway maintained by the appropriate CMS provider (CMS Provider Gateway).³¹ Each individual CMS Provider Gateway would be responsible for the management of the particular CMS provider elections to deliver alerts. The CMS Provider Gateway would also be responsible for formulating the alert in a manner consistent with the individual CMS provider's available delivery technologies, mapping the alert to the associated set of cell sites/paging transceivers, and handling congestion within the CMS provider infrastructure. Ultimately, the alert would be received on a customer's mobile device. The major functions of the mobile device would be to authenticate interactions with the CMS provider infrastructure, to monitor for CMAS alerts, to maintain customer options (such as the subscriber's opt-out selections), and to activate the associated visual, audio, and mechanical (e.g., vibration) indicators that the subscriber has indicated as options when an alert is received on the mobile device.³² As part of its recommended model, the CMSAAC also proposed technical standards defining the functions of the Alert Aggregator, Alert Gateway, CMS Provider Gateway, CMS infrastructure, CMS handsets and various interfaces (i.e., A, B, C, D and E interfaces).³³

11. In the *CMAS NPRM*, we sought comment on the CMSAAC's proposed reference architecture, including its standards for defining the various element functions.³⁴ Although most commenters supported the CMSAAC's proposal, a few objected to the CMSAAC's recommendation concerning the government-administered Alert Aggregator and an Alert Gateway. The Association of Public Television Stations (APTS) suggested that the Commission's role under the WARN Act is limited to adopting protocols to enable mobile services to opt into the Digital Emergency Alert System (DEAS).³⁵ CellCast asserted that a national Aggregator/Gateway is not required for CMAS implementation and that there are multiple models for alert distribution that do not use such an element.³⁶ DataFM and the National Association of Broadcasters (NAB) raised concerns that a national aggregator would create a single point of failure that would reduce CMAS resiliency and/or introduce unacceptable performance degradation.³⁷

12. According to the CMSAAC, a key element to CMS providers' ability to participate in the CMAS is the assumption of the Alert Aggregator and Alert Gateway functions by a Designated Federal

³⁰ See CMSAAC recommendations, § 2.3.1.

³¹ See CMSAAC recommendations, § 2.3.2.

³² See CMSAAC recommendations, § 2.3.5.

³³ Each interface in the CMSAAC Reference Architecture represents a place where two elements in the Reference Architecture meet or connect. The "A" interface represents that connection between the alert initiator and the Alert Aggregator, the "B" interface represents the connection between the Alert Aggregator and Alert Gateway, the "C" interface represent the connection between the Alert Gateway and the CMS Provider Gateway, the "D" interface represents the connection between the CMS Provider Gateway and the CMS provider infrastructure, and the "E" interface represents the connection between the CMS provider infrastructure and the mobile device. For the purposes of this Order, the most important interfaces are the "C" and "E" interfaces. The "C" interface requires common protocols that will ensure that the alert information that flows from the Federal government administered Alert Gateway and the CMS providers is secure and accurate. Accordingly, both the Alert Gateway and CMS Provider Gateway must operate under a common set of protocols. The "E" interface will determine what information will appear on the mobile device. It is essential that the requirements for this interface allow accurate, timely, and accessible alerts for the mobile device user.

³⁴ See *CMAS NPRM*, 22 FCC Rcd at 21979-80, ¶¶ 12-13.

³⁵ See APTS Comments at 2-3. The Digital Emergency Alert System (DEAS) is a next generation alert and warning system that leverages the transition of television to DTV format.

³⁶ See CellCast Comments at 24.

³⁷ DataFM Comments at 10, NAB Comments at 2-3.

Government Entity.³⁸ Specifically, the CMSAAC recommended that the CMAS channel all Commercial Mobile Alert Messages (CMAMs) submitted by Federal, State, Tribal and local originators through a secure, Federal government administered, CAP-based alerting framework that would aggregate and hand off authenticated CMAMs to CMS Provider Gateways.³⁹ We sought comment on this recommendation in the *CMAS NPRM*.⁴⁰ The overwhelming majority of commenting parties supported the CMSAAC's recommendation.⁴¹ Most wireless carriers commenting on the issue stressed that this was essential to CMS providers' participation in the CMAS. ALLTEL, for example, stated that if "a federal government entity does not assume these roles, wireless service providers are less likely to participate" in the CMAS because "in an emergency situation it is imperative that wireless service providers are able to rely on a single source . . . and government officials are more appropriately trained in authenticating and constructing messages."⁴²

13. We adopt the CMSAAC's proposed architecture for the CMAS.⁴³ We find that the recommended model will facilitate an effective and efficient means to transmit alerts and find that the public interest will be served as such. Contrary to APTS's assertions, nothing in section 602(a) of the WARN Act mandates that we only adopt requirements for CMS providers to opt into DEAS.⁴⁴ While we agree with CellCast that there are other potential models for alert delivery by electing CMS providers, we note that none of those alternative solutions received the support of the CMSAAC. Moreover, we note that the CMSAAC recommendation is the result of consensus among commercial wireless carriers and their vendors, public safety agencies, organizations representing broadcast stations and organizations representing people with disabilities and the elderly, and other emergency alert experts. This consensus was reached after approximately ten months of deliberation. No other party has suggested an alternative that would be superior in meeting the needs of the commercial wireless industry and in ensuring that alerts are received by electing CMS providers and then are transmitted to their subscribers. In fact, both during the CMSAAC deliberations as well as throughout this proceeding, many wireless carriers have indicated that the inclusion of an alert aggregator and alert gateway function is essential to their participation in the voluntary CMAS.⁴⁵

³⁸ See CMSAAC recommendations, § 2.2.

³⁹ See CMSAAC recommendations, § 2.2.2

⁴⁰ *CMAS NPRM*, 22 FCC Rcd at 21979-80, ¶¶ 12-13.

⁴¹ See generally, Alltel Communications LLC (Alltel) Comments at 4, AT&T Inc. (AT&T) Comments at 6, T-Mobile Comments at 7, and the California Public Utilities Commission (CAPUC) Comments at 6,7. *But see, e.g.*, Ken Post Comments at 2 (CMAS should be based on a shared authority system as envisioned by the National Incident Management System), National Association of Broadcasters (NAB) Comments at 2-3 (a government-run aggregator creates a complex single system that has the potential to be a single point of failure), CellCast Comments at 7-9 (aggregator is not required for CMAS implementation, either at the National, State, or local levels).

⁴² Alltel Comments at 4.

⁴³ See CMSAAC recommendations, §§ 2.3.5 and 7.

⁴⁴ As noted, *infra* at ¶¶ 34-41 the CMSAAC recommendations and this First Report and Order consistently conclude that the requirements for the CMAS should be technologically neutral. APTS's arguments regarding equipment are more appropriately addressed in the order that addresses section 602(c) of the WARN Act.

⁴⁵ AT&T Comments at 6 ("it is critical to the success... that a single Government Entity serve as the alert aggregator and gateway... whether it assumes this role directly or via a third party contractor"); CTIA Comments at 2 (Commission adoption of the CMSAAC recommendations as submitted will encourage the highest level of participation); T-Mobile Comments at 15, 16 (Centralization is key to the proper functioning of a CMAS, and that it must be managed by the federal government. Without the centralized system, participation at all these levels could result in chaos).

14. Finally, we disagree with the concerns raised by DataFM and NAB that a national aggregator would necessarily create a single point of failure. While the CMSAAC recommended a single logical aggregator/gateway function, we expect that these functions will be implemented in a reliable and redundant fashion to maximize resiliency.⁴⁶ Furthermore, given the volume of alerts expected for the CMAS, we believe that technology for processing alerts will not place a constraint on aggregator/gateway performance.⁴⁷ Accordingly, we adopt the architecture proposed by the CMSAAC. As described below, however, we adopt as rules only those CMAS elements within the control of the CMS providers.

15. *Federal Government Role.* We agree with the CMSAAC and the majority of commenters that a Federally administered aggregator/gateway is a necessary element of a functioning CMAS. While no Federal agency has yet been identified to assume these two functions,⁴⁸ we believe that a Federal government aggregator/gateway would offer the CMS providers the best possibility for the secure, accurate and manageable source of CMAS alerts that the WARN Act contemplates.

16. We believe that FEMA, some other entity within DHS, or NOAA may be in the best position to perform these functions.⁴⁹ DHS, and more specifically FEMA, traditionally has been responsible for origination of Presidential alerts and administration of the EAS.⁵⁰ Moreover, Executive Order 13407 gives DHS primary responsibility for implementing the United States' policy "to have an effective, reliable, integrated, flexible and comprehensive system to alert and warn the American people in situations of war, terrorist attack, natural disaster or other hazards to public safety and well-being."⁵¹ By the same token, the Department of Commerce, and more specifically NOAA Weather Radio, as the "All Hazards" radio network, acts as the source for weather and emergency information, including natural

⁴⁶ See CMSAAC recommendations at 71. The CMSAAC recommended that CMAS system reliability meet "telecom standards for highly reliable systems," which generally implies the use of redundant elements where single points of failure would otherwise exist.

⁴⁷ Based on the CMAS alert volumes anticipated by the CMSAAC in section 11 of the CMSAAC recommendations, we agree with the CMSAAC's view that developing the technology for processing alerts according to the CMSAAC proposed timeline will not overburden the aggregator/gateway performance.

⁴⁸ See FEMA Comments at 2 (stating that although it supports the CMSAAC's recommendations, it "[do[es] not have the authority during non-emergency periods to develop, implement, operate or maintain elements of the CMAS that regard alerts, warnings or notifications originated by state and local authorities such as the Aggregator and Gateway functions of the Trust Model of the CMAS, under [its] current statutory authority.")

⁴⁹ FEMA administers the Emergency Alert System (EAS) while NOAA operates the NOAA Weather Radio (NWR). See <http://www.weather.gov/nwr/> (last viewed on April 7, 2008). The respective roles of the Commission, FEMA, and NOAA are based on a 1981 Memorandum of Understanding, see *State and Local Emergency Broadcasting System (EBS) Memorandum of Understanding Among the Federal Emergency Management Agency (FEMA), Federal Communications Commission (Commission), and the National Oceanic and Atmospheric Administration (NOAA)* (Approved by National Industry Advisory Committee (NIAC) on April 21, 1982), a 1984 Executive Order, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, Exec. Order No. 12,472, 49 Fed. Reg. 13,471 (1984), and a 1995 Presidential Statement of Requirements, see *Presidential Communications with the General Public During Periods of National Emergency*, The White House (September 15, 1995).

⁵⁰ While the FCC could perform this role, additional funding to support such an undertaking would likely be necessary. We note that unlike the FCC, DHS and the Department of Commerce have authority under the WARN Act to borrow up to \$106 million against Digital Television (DTV) transition revenues in order to fulfill their obligations under the statute. See WARN Act, § 606(c). It is also our understanding that FEMA has funding for its Integrated Public Alert and Warning System.

⁵¹ Executive Order 13407, § 1.

(such as earthquakes or avalanches), environmental (such as chemical releases or oil spills), and public safety (such as AMBER alerts or 911) warning information.⁵²

17. FEMA also played an integral role in the development of the CMSAAC's recommendations. FEMA chaired the Alert Interface Group (AIG), which was responsible for addressing issues at the front-end of the CMAS architecture (e.g., receipt and aggregation of alerts, development of trust model to authenticate alerts from various sources). It also represented the AIG before the CMSAAC Project Management Group (PMG), which coordinated the work of all the other CMSAAC working groups and assembled the CMSAAC recommendations document. In addition, FEMA voted to adopt the CMSAAC recommendations in October 2007, which included CMAS reliance on a single Federal authority to fulfill the gateway/aggregator role.

18. We recognize that FEMA asserted in its February 2008 comments that limits on its statutory authority preclude the agency from fulfilling the Federal aggregator/gateway functions.⁵³ Nevertheless, timely identification of a federal agency capable of fulfilling the aggregator/gateway functions recommended by the CMSAAC is essential to bringing the concrete public safety benefits of a CMAS system to the American people.⁵⁴ We are hopeful that any bars that prevent FEMA or some other entity within DHS from fulfilling these roles will be lifted expeditiously. We will work with our Federal partners and Congress, if necessary, to identify an appropriate government entity to fulfill these roles, whether that is FEMA, another DHS entity, NOAA or the FCC.

19. *Scope of Order.* Accordingly for purposes of this Order, we proceed on the assumption that a Federal agency will assume these roles at a future date. Today's Order is limited to adopting rules governing those sections of the CMAS architecture that are within the control of electing CMS providers.⁵⁵ These include rules regarding the CMS Provider Gateway, CMS provider infrastructure, and CMS provider handsets. Specifically, we adopt rules, based on the CMSAAC's recommendations, that require each individual CMS Provider Gateway to be able to receive alerts from the Federal government alert gateway over a secure interface (i.e., "C Interface").⁵⁶ The CMS Provider Gateway will be required to, among other things: (1) manage the CMS provider's election to provide alerts; (2) format alerts

⁵² FEMA administers the Emergency Alert System (EAS) while NOAA operates the NOAA Weather Radio (NWR). See <http://www.weather.gov/nwr/> (last viewed on April 7, 2008). The respective roles of the Commission, FEMA, and NOAA are based on a 1981 Memorandum of Understanding, *see State and Local Emergency Broadcasting System (EBS) Memorandum of Understanding Among the Federal Emergency Management Agency (FEMA), Federal Communications Commission (Commission), and the National Oceanic and Atmospheric Administration (NOAA)* (Approved by National Industry Advisory Committee (NIAC) on April 21, 1982), a 1984 Executive Order, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, Exec. Order No. 12,472, 49 Fed. Reg. 13,471 (1984), and a 1995 Presidential Statement of Requirements, *see Presidential Communications with the General Public During Periods of National Emergency*, The White House (September 15, 1995).

⁵³ See FEMA Comments at 2.

⁵⁴ Accordingly, the compliance date for the rules we adopt today is tied to the announcement of an entity to fulfill these functions. The absence of an aggregator/gateway, however, will have no impact on a CMS provider's obligation under the WARN Act to elect whether or not it intends to transmit emergency alerts within 30 days of the Commission's issuance of rules required under section 602(b). See WARN Act, § 602(b).

⁵⁵ A complete list of the required CMS infrastructure functions is set forth in the rules in Appendix C.

⁵⁶ The C interface is a secure interface over which alerts can be passed from the Aggregator/Gateway to the CMS Provider Gateway. Under our rules, the CMS provider must: (1) provide information for the authentication and validation of actions across the interface; (2) be able to receive new, updated or cancelled wireless alert messages from the Alert Gateway in a format that is suitable for the mobile devices and the wireless alert deliver technology or technologies implemented by the CMS provider; and (3) acknowledge the receipt of new, updated or cancelled wireless alert messages.

received in a manner consistent with the CMS provider's available delivery technology; (3) map alerts to the associated set of cell sites/paging transceivers; and (4) manage congestion within the CMS provider's infrastructure.⁵⁷ In addition, we adopt rules, based on the CMSAAC's recommendations, requiring the CMS infrastructure to, among other things: (1) authenticate interactions with the mobile device; (2) distribute received CMAS alert messages to the appropriate set of cell sites/paging transceivers for transmission to the mobile device; and (3) transmit the CMAS alert message for each specified cell site/pager transceiver.⁵⁸

20. We adopt the CMSAAC's recommendations regarding capabilities of the mobile device including that it: (1) authenticate interactions with the CMS provider infrastructure; (2) maintain configuration of CMAS alert options; and (3) present received CMAS alert content to the subscriber.⁵⁹ In addition, as explained below, we adopt requirements for the mobile device to ensure that people with disabilities are able to receive CMAS alerts.⁶⁰ We also adopt the CMSAAC's recommendation that CMAS alerts not preempt ongoing voice or data sessions.⁶¹

21. In keeping with our policy to promote technological neutrality, we decline to adopt rules governing the communications protocols that the CMS providers must employ for communications across the D or E interfaces as identified in the architecture.⁶² We agree with the CMSAAC that no specific protocols should be required for the D and E interface, but rather that CMS providers should be allowed to retain the discretion to define these protocols in conjunction with their overall network design and with the mobile device vendors.⁶³ Both of these interfaces lie entirely within the control of the CMS providers and any implementation decisions there will have no impact on CMAS ability to satisfy the system requirements we set forth elsewhere in this Order.⁶⁴ For example, while we do include requirements on the type of alert information that must cross the D and E interfaces to enable CMAS alerts on mobile devices, we choose to remain silent as to the precise communications protocol that a CMS provider uses to convey this information to the mobile device.⁶⁵ This approach gives the CMS providers maximum flexibility to leverage technological innovation and implement the CMAS in a cost effective manner.

22. We also adopt rules requiring, per the CMSAAC's recommendation, that electing CMS providers assemble individual profile information to provide to the Authorized Federal Government Entity, once that entity is identified.⁶⁶ We believe that electing CMS providers expect to assemble this

⁵⁷ A complete list of the CMS Provider Gateway's required functions is set forth in the rules in Appendix C.

⁵⁸ Interstate Wireless supports the CMSAAC recommended reference architecture, but notes that the cost of building and maintaining a CMS Provider Gateway would be more than it and other similarly situated Small Business CMS providers could afford and still be able to provide the alert service to the public without cost. Accordingly, Interstate Wireless requests that the Federal Government either provide the proper software and reception equipment for the CMS Provider Gateways, or provide grants to the Small Business CMS providers to purchase, install, and maintain the equipment themselves. Interstate Wireless Comments at 6. We acknowledge the concern of Interstate Wireless, but note that questions of funding are not addressed by section 602(a) of the WARN Act, and thus are outside of the scope of this order.

⁵⁹ CMSAAC recommendations, § 1.1.1.

⁶⁰ See *infra* ¶¶ 57-67.

⁶¹ CMSAAC recommendations, § 7.3.

⁶² See Functional Reference Model Diagram, *supra* ¶ 10.

⁶³ No commenter objected to this recommendation.

⁶⁴ For this reason, we conclude that our decision is consistent with section 602(a) of the WARN Act which requires that we adopt technical requirements "necessary" for CMS alerting capability. WARN Act, § 602(a).

⁶⁵ See *infra*, ¶¶ 26-30 (discussion of CMAS Alert Categories).

⁶⁶ See CMSAAC recommendations, § 2.2.4.2.

information, and by adopting this requirement now, we are providing direction to potential Alert Gateway providers.⁶⁷

23. The CMSAAC recommended detailed technical protocols and specifications for the Alert Aggregator/Gateway entity and the CMS providers to employ for the delivery of alerts over the various interfaces (*i.e.*, A, B and C interfaces) in the Reference Model. Specifically, section 10 of the CMSAAC recommendations proposed requirements that Alert Initiators must meet to deliver CMAS alerts to the Alert Aggregator, and that the Alert Gateway must meet to deliver CMAS alerts to the CMS Provider Gateway.⁶⁸ The CMSAAC also recommended CAP-based mapping parameters.

24. We support the technical protocols and specifications for the delivery of alerts recommended by the CMSAAC in this section. Electing CMS providers could use these technical protocols and specifications to design their internal systems that would enable compliance with the rules we adopt in this docket. We decline, however, to codify these protocols and specifications in this Order. We believe that these protocols offer a significant guidance to CMAS participants as they further develop the final protocols and interface for the CMAS, but until an Alert Aggregator/Gateway entity is determined, additional refinements and revisions of these protocols and specifications are inevitable. Accordingly, we conclude that final determination of these interface protocols is better left to industry standards organizations.⁶⁹ We will revisit this matter in the future if Commission action in this area is indicated.

C. General CMAS Requirements

25. In this section, we establish the basic regulatory framework of the new CMAS. Specifically, we adopt technologically neutral rules that address, among other things, the scope of CMAS alerts, geo-targeting and alert accessibility for people with disabilities and the elderly.

1. Scope and Definition of CMAS Alerts

26. The WARN Act requires the Commission to enable commercial mobile alerting capabilities for "emergency" alerts,⁷⁰ but does not define what may comprise an emergency. Accordingly, in the *CMAS NPRM*, we sought comment on the appropriate scope of emergency alerts, including whether and to what extent alerts should be classified.⁷¹ We specifically asked parties to address whether we should implement the CMSAAC's recommendation to specify three alert classes: (1) Presidential Alert; (2) Imminent Threat Alert; and (3) Child Abduction Emergency or AMBER Alert.⁷² For the reasons stated below, we find that the public interest will be best served by our adopting these three alert classes, and we define them below.

27. We agree with the majority of commenters that the three classes of alert recommended by the CMSAAC achieves the best balance between warning of imminent threat to life and property with the current technical limits that CMS provider systems face in delivering timely, accurate alerts.⁷³ Alert

⁶⁷ See CMSAAC recommendations, § 2.2.4.2 and Table 2.1.

⁶⁸ See CMSAAC recommendations, § 10.

⁶⁹ We note that the Alliance for Telecommunications Industry Solutions (ATIS) and Telecommunications Industry Association (TIA) are beginning to engage in standards setting related to the CMAS. See ATIS Comments at 4-5.

⁷⁰ WARN Act, § 602(b)(2)(e).

⁷¹ *CMAS NPRM*, 22 FCC Rcd at 21981, ¶16.

⁷² *Id.*

⁷³ CMSAAC recommendations at § 5.1. See also CAPUC Comments at 10-11.

Systems however argues that we should include additional classes of alerts, such as traffic advisories.⁷⁴ We find that inclusion of such alerts would be inconsistent with the intent of Congress, expressed throughout the WARN Act, that the Commission enable an “emergency” alerting system. We believe that if the public were to receive commercial mobile alerts that do not relate to *bona fide* emergencies, there would be a serious risk that the public would disregard mobile alerts or possibly opt not to receive anything but Presidential alerts.⁷⁵ We also note that, given the current technical capabilities of CMS providers to deliver emergency alerts, it is possible that if too many alerts are injected into a CMS provider’s system in a very brief period, vital messages could be delayed. Accordingly, we reject arguments to broadly define eligible alert classes beyond those specified here.

a. Presidential Alerts

28. Section 602(b)(2)(E) of the WARN Act authorizes participating CMS providers to allow device users to prevent the receipt of alerts or classes of alerts “other than an alert issued by the President.”⁷⁶ Congress thus intended to afford Presidential Alerts the highest priority. Affording Presidential Alerts the highest priority also will enable the Secretary of Homeland Security to meet his/her obligation, under Executive Order 13407, to “ensure that under all conditions the President of the United States can alert and warn the American people.”⁷⁷ Accordingly, electing CMS providers must transmit such alerts and assign the highest priority to any alert issued by the President or the President’s authorized designee.⁷⁸ Further, Presidential Alerts must be transmitted upon receipt by a CMS provider, without any delay, and therefore will preempt any other pending alert. We note that due to the initial 90-character text message protocol that we are adopting below for the first generation CMAS,⁷⁹ it is possible that a Presidential Alert may direct recipients to other sources, possibly taking the form recommended by the CMSAAC: “The President has issued an Emergency Alert. Check local media for more details.”⁸⁰

b. Imminent Threat Alerts

29. We note that virtually all commenting parties support adoption of the CMSAAC’s recommendation to define an Imminent Threat Alert class.⁸¹ This alert class is narrowly tailored to those emergencies where life or property is at risk, the event is likely to occur, and some responsive action should be taken. Specifically, an Imminent Threat Alert must meet separate thresholds regarding urgency, severity, and certainty. Each threshold has two permissible CAP values.

- Urgency. The CAP “urgency” element must be either Immediate (*i.e.*, responsive action should be taken immediately) or Expected (*i.e.*, responsive action should be taken soon, within the next hour).⁸²
- Severity. The CAP “severity” element must be either Extreme (*i.e.*, an extraordinary threat to

⁷⁴ Alert Systems Comments at 16 (urging more than three classification levels, claiming disaster managers need the ability to dispatch road closure and other community relevant information).

⁷⁵ See MetroPCS Comments at 3 (noting that if too many alert messages are transmitted, users may ignore them); T-Mobile Comments at 10 (“[s]ubscribers will be more likely to opt out of CMAS altogether if their devices are inundated with minor alerts”).

⁷⁶ WARN Act, § 602(b)(2)(e).

⁷⁷ Executive Order 13407, § 2(a)(x).

⁷⁸ See CMSAAC recommendations, § 2.3.2 (CMS providers will prioritize Presidential alerts).

⁷⁹ See *infra* ¶¶ 82-83.

⁸⁰ CMSAAC recommendations, § 5.3.3.

⁸¹ *But cf.* CellCast Comments at 29 (opposing adoption of alert classes).

⁸² See CAP-V1.1 at 16.

life or property) or Severe (*i.e.*, a significant threat to life or property).⁸³

- Certainty. The CAP “certainty” element must be either Observed (*i.e.*, determined to have occurred or to be ongoing) or Likely (*i.e.*, has a probability of greater than fifty percent).⁸⁴ That is, the event must have occurred, or be occurring (Observed), or be more likely to occur than not (Likely).

30. We find that the transmission of these imminent threat alerts is essential to a useful CMAS. The CMSAAC recommended such action and the commenting parties overwhelmingly support this conclusion.⁸⁵ As T-Mobile correctly states, CMAS alerts are not appropriate for warning the public about minor events.⁸⁶ Subscribers are more likely to opt out if they are bombarded by minor notices, and may fail to notice a truly serious alert. Also, inclusion of minor events would be an unnecessary burden on the CMS provider infrastructure. Accordingly, we find it appropriate to require participating CMS providers to transmit Imminent Threat Alerts,

c. Child Abduction Emergency/AMBER Alerts

31. There is broad support in the record for adoption of the CMSAAC’s recommendation to specify a third alert class, Child Abduction Emergency or AMBER Alert.⁸⁷ There are four types of AMBER Alerts: (1) Family Abduction,⁸⁸ (2) Nonfamily Abduction,⁸⁹ (3) Lost, Injured, or Otherwise Missing,⁹⁰ and Endangered Runaway.⁹¹ AMBER plans are voluntary partnerships between law enforcement agencies, broadcasters and CMS providers to activate an urgent bulletin in the most serious child abduction cases, and AMBER alerts are issued only where an AMBER plan has been duly established.⁹² We also note that a number of CMS providers currently transmit AMBER Alerts using

⁸³ See CAP-V1.1 at 17.

⁸⁴ *Id.*

⁸⁵ See *supra*, n.20.

⁸⁶ T-Mobile Comments at 9-10.

⁸⁷ See, e.g., Acision Comments at 6-7 (supporting the inclusion of AMBER alerts to, among other things, maintain public awareness of the CMAS). We note that on April 30, 2003, President George W. Bush signed the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today (PROTECT) Act of 2003 (Pub. L. No. 108-21, 117 Stat 650 (Apr. 20, 2003)) into law. Building on the steps already taken by the Federal Government to support AMBER Alerts, this Act codified the national coordination of state and local programs, including the development of guidance for issuance and dissemination of AMBER Alerts and the appointment of a national AMBER Alert Coordinator.

⁸⁸ A Family Abduction (FA) involves an abductor who is a family member of the abducted child such as a parent, aunt, grandfather, or stepfather. See <http://www.amberalert.gov/statistics.htm>.

⁸⁹ A Nonfamily Abduction (NFA) involves an abductor unrelated to the abducted child, either someone unknown to the child and/or the child’s family or an acquaintance/friend of the child and/or the child’s family. *Id.*

⁹⁰ A Lost, Injured, or Otherwise Missing (LIM) involves a case where the circumstances of the child’s disappearance are unknown. *Id.*

⁹¹ An Endangered Runaway (ERU) involves a missing child who is believed to have run away and in imminent danger. *Id.*

⁹² Localities generally establish AMBER plans based on the U.S. Department of Justice’s five criteria that should be met before an alert is activated: (1) law enforcement confirms a child has been abducted; (2) the child is 17 years or younger; (3) law enforcement believes the child is in imminent danger of serious bodily harm or death; (4) there is enough descriptive information about the victim and the abduction to believe an immediate broadcast alert will help; and (5) the child’s name and other data have been entered into the National Crime Information Center. See <http://www.amberalert.gov/>.

Short Message Service (SMS) technology,⁹³ and we applaud their potentially life-saving efforts in this regard.

32. In 2006, 261 AMBER Alerts were issued in the United States involving 316 children.⁹⁴ Most of these alerts were issued on an intrastate basis.⁹⁵ Of the 261 AMBER Alerts issued in 2006, 214 cases resulted in a recovery, 53 of which were resolved as a direct result of an AMBER Alert being issued.⁹⁶ Based on the limited number of AMBER alerts and their confined geographic scope, we do not expect such alerts to be overly burdensome to CMS providers that participate in the CMAS. Moreover, because of the efficacy of AMBER Alerts, we find that the public interest in the safety of America's children will be well served by the provision of AMBER Alerts by the wireless industry. Accordingly, we require participating CMS providers to transmit AMBER alerts.

2. Technologically Neutral Alert System

33. The CMSAAC recommended that CMS providers that elect to participate in the CMAS should "not be bound to use any specific vendor, technology, software, implementation, client, device, or third party agent, in order to meet [their] obligations under the WARN Act."⁹⁷ We agree. As SouthernLINC notes, participating CMS providers should be able to choose the technology that will allow them to best meet the emergency alerting needs of the American public.⁹⁸ Consistent with the Commission's well-established policy of technologically-neutral regulation of the wireless telecommunications industry,⁹⁹ we believe that CMS providers and equipment manufacturers are in the best position to select and incorporate the technologies that will enable them to most effectively and efficiently deliver mobile alerts. Accordingly, we will not limit the range of technologies that electing CMS providers may deploy to participate in the CMAS. In reaching this conclusion, we have balanced the alerting needs of the public and the capabilities of electing CMS providers and our mandate under section 602(a) of the WARN Act to enable the provision of emergency alerts.¹⁰⁰ We emphasize that the WARN Act does not require the establishment of any specific technology to be used for the CMAS.

34. CMS providers are in various stages of readiness to participate in the CMAS. Paging carriers already provide point to multipoint services, using technologies such as ReFLEX and POCSAG (Post Office Code Standardization Advisory Group), to reach many subscribers at the same time and therefore appear well-positioned to participate in CMAS.¹⁰¹ However, as the American Association of

⁹³ See *How Wireless AMBER Alerts™ Are Sent*, available at <http://wirelessamberalerts.adcouncil.org/howwirelessamberalertswork.htm>.

⁹⁴ See National Center for Missing & Exploited Children, 2006 *AMBER-Alert Report* at 7.

⁹⁵ In 2006, 11 AMBER Alerts were extended beyond the limits of the state where the alert first originated. *Id.* at 8. Eight alerts were extended to one additional state, and three alerts were extended to two states each. *Id.*

⁹⁶ Nine (9) children were recovered deceased, and, as of April 21, 2007, 10 cases remained active with 11 children still missing. *Id.*

⁹⁷ CMSSAC recommendations, §5.1.

⁹⁸ SouthernLINC Comments at 4-6.

⁹⁹ See Amendment of the Commission's Rules to Permit Flexible Service Offerings in the Commercial Mobile Radio Services, WT Docket No. 96-6, *Second Report and Order and Order on Reconsideration*, 15 FCC Rcd 14680 (2000).

¹⁰⁰ WARN Act, § 602(a).

¹⁰¹ ReFLEX is a wireless network protocol developed by Motorola which is used for two-way paging. Narrowband PCS carriers use the ReFLEX technology protocol, which can transmit data at speeds ranging from 3.2 to 25 kbps. See *Tenth CMRS Competition Report*, 20 FCC Rcd at 15955, ¶ 124. For more information regarding ReFLEX, see <http://usamobility.com/pdf/ReFLEX2.pdf>. For more information regarding POCSAG, see <http://www.wireless.per.nl/reference/chaptr01/dtmmysyst/paging.htm>.

Paging Carriers notes, it may not be feasible for paging carriers to confine their alerts to either county-wide or sub-county distribution.¹⁰² Further, cellular, PCS, and SMR service providers, report that they have not deployed an emergency alerting capability that satisfies all requirements in the CMSAAC recommendations and that is currently available for the mass transmission of alerts.¹⁰³ We note that many of the requirements that we adopt today are intended to apply to a first generation text-based alerting service. Other service profiles, such as streaming audio and video, are in their early developmental stages and thus not ripe for implementation by the Commission. We foresee that as CMS providers gain experience with these and other alerting technologies, they may well be incorporated into future alerting system deployments.

35. Although the CMSAAC found that point-to-point technologies may not be well suited for mass alerting,¹⁰⁴ we will not prohibit their use if a CMS provider can otherwise meet the requirements that we establish today. Short Message Service (SMS)¹⁰⁵ text messaging is available to most cellular, PCS, and SMR subscribers and is currently used by some municipalities and other local jurisdictions to provide emergency alerts on an opt-in basis.¹⁰⁶ We recognize, however, that SMS may not be a desirable solution for the widespread dissemination of alerts to the public because the mass delivery of SMS-formatted alerts could degrade network performance and delay alert delivery. Despite these potential drawbacks, SMS text messaging may offer a viable, short-term delivery method for electing CMS providers that do not yet have a point-to-multipoint text messaging capability.¹⁰⁷

36. The CMSAAC noted that technologies such as MediaFLO and DVB-H “may provide supplemental alert information,”¹⁰⁸ but recommended that they should not be considered as part of the CMAS.¹⁰⁹ Our goal in this proceeding is to enable the broadest possible voluntary participation in the CMAS, and we will not foreclose the possible deployment of these or other innovative technologies as a means of participating in the nascent CMAS. The public interest is best served by not circumscribing the range of technologies that CMS providers may elect to deploy to meet the alerting needs of the American public.

¹⁰² See AAPC Comments at 7.

¹⁰³ See, e.g., Sprint Nextel Comments at 8-9 (noting that certain industry standardization processes must be completed before CMAS deployment).

¹⁰⁴ According to the CMSAAC, point-to-point technologies may experience delivery delays, network congestion, and lack geo-targeting capabilities because alerts are targeted to phone numbers instead of a specific alert area. See CMSAAC recommendations at § 5.2.

¹⁰⁵ SMS enables the transmission of alphanumeric messages between mobile subscribers and external systems such as electronic mail, paging, and voice mail systems. For a more complete description, see <http://electronics.howstuffworks.com/sms1.htm> and http://www.mobilein.com/SMS_tutorial.pdf.

¹⁰⁶ The District of Columbia and many of its neighboring jurisdictions, for example, have such emergency alert systems. See <http://textalert.ema.dc.gov> (Alert DC); <http://www.fairfaxcounty.gov/cean> (Fairfax County, VA); <http://alert.montgomerycountymd.gov> (Montgomery County, MD).

¹⁰⁷ Many CMS providers are successfully using SMS today to transmit geographically specific AMBER Alerts to interested subscribers. The wireless AMBER alert system notifies wireless customers who have elected to receive the service of missing children alerts. Information regarding the system is available at <http://www.wirelessfoundation.org/amber>. Thirty-two wireless carriers currently participate in the system. See <http://wirelessamberalerts.adcouncil.org/partners.htm>.

¹⁰⁸ CMSAAC recommendations, § 5.2. Information regarding MediaFLO technology is available at http://www.qualcomm.com/mediaflo/about_us/index.shtml. Information regarding DVB-H technology is available at <http://www.dvb-h.org/technology.htm>.

¹⁰⁹ CMSAAC recommendations, § 5.2.

37. Several parties express support for an FM-based CMAS solution such as that provided by ALERT-FM and Global Security Systems.¹¹⁰ The CMSAAC however considered the costs and benefits of Radio Broadcast Data System (RBDS) and other FM-based alert and warning solutions, and found them to be infeasible for the CMAS.¹¹¹ Moreover, a number of parties have expressed reservations about these technologies.¹¹² Nonetheless, in keeping with our overall policy to maintain technological neutrality, we do not require or prohibit the use of ALERT-FM, RBDS or similar systems as the basis of the CMAS.¹¹³

38. We also strongly encourage fair, reasonable, and nondiscriminatory Intellectual Property Rights (IPR) licensing in the context of the CMAS. We agree with the CMSAAC that the technical standards, protocols, procedures, and related requirements that we adopt pursuant to section 602(a) of the WARN Act today should be standardized in industry bodies that have well defined IPR policies.¹¹⁴ We decline, however, to compel all CMSAAC participants “to provide written assurance to the Commission that, if and insofar as one or more licenses may be required under any of their respective IPRs that are technically essential for purposes of implementing or deploying CMAS, the rights holders shall license such IPR on a fair, reasonable and nondiscriminatory basis for those limited purposes only.”¹¹⁵ We also decline to require “all participants in the public comment process on th[e] CMAS Architecture and Requirements document” to make such a written assurance.¹¹⁶ These requests are outside the scope of section 602(a) of the WARN Act.

39. The CMSAAC made a number of additional recommendations that we conclude are outside the scope of our mandate under section 602(a) of the WARN Act to adopt “technical standards, protocols, procedures, and other technical requirements,” to enable voluntary commercial mobile alerting.¹¹⁷ Specifically, the CMSAAC submitted recommendations regarding the applicability of requirements for location, number portability and the Communications Assistance for Law Enforcement Act (CALEA).¹¹⁸ The CMSAAC also submitted recommendations on whether CMS providers may utilize the technical requirements adopted herein for other services and purposes and whether CMS providers may recover certain costs related to the development of the CMAS.¹¹⁹ We find that these issues are outside the scope of section 602(a) of the WARN Act and, therefore, do not address these issues herein.

40. The CMSAAC recommended that, to the extent practicable, “Federal, state, tribal, and local level CMAS alert messages [should] be supported using the same CMAS solution.”¹²⁰ We agree. We believe that a uniform approach to implementation of the CMAS will be inherently more cost

¹¹⁰ See, e.g., Comments of Data-FM at 7-8, Sheriff of Jefferson County, Louisiana; Florida Association of Broadcasters, Mississippi Office of Homeland Security, Mississippi Office of Emergency Management.

¹¹¹ See CMSAAC recommendations at 47-48.

¹¹² See e.g., AT&T Reply Comments at 11-12.

¹¹³ CMS providers have discretion to use these technologies so long as they are able to transmit emergency alerts in a manner consistent with the rules we adopt today.

¹¹⁴ CMSAAC recommendations, § 5.1.

¹¹⁵ *Id.*

¹¹⁶ *Id.*

¹¹⁷ WARN Act, § 602(a).

¹¹⁸ CMSAAC recommendations, § 5.2.4.

¹¹⁹ CMSAAC recommendations, § 5.1

¹²⁰ *Id.*

effective, more technologically consistent and thus more likely to facilitate participation by small and rural CMS providers. Further, we agree that electing CMS providers should not be required to support alerting on mobile handsets manufactured for sale to the public prior to a CMS provider's initiation of the CMAS alerting service. In a subsequent order, we will address how participating CMS providers may sell such non-compliant handsets consistent with the requirement under section 602(b) of the WARN Act that they disclose "at the point of sale of any devices with which its commercial mobile service is included, that it will not transmit such alerts via the service it provides for the device."¹²¹ Finally, we agree that electing CMS providers should have discretion regarding whether certain devices, such as laptop wireless data cards, will support alerting capabilities.

3. CMAS Message Elements and Capabilities

a. Required Alert Message Elements

41. The CMSAAC recommended that emergency alert messages follow the same general format of National Weather Service alert messages, subject to a 90-character text limitation.¹²² Specifically, the CMSAAC recommended that for initial CMAS deployments, messages should include five elements in the following order:

- Event Type or Category
- Area Affected
- Recommended Action
- Expiration Time (with time zone)
- Sending Agency

The CMSAAC proposed this format to facilitate CAP value field mapping to text.¹²³ It also noted that the format would likely evolve as experience is gained by alert initiators and by electing CMS providers.¹²⁴ In the *CMAS NPRM*, we sought comment on the five elements and asked parties to address whether the elements are consistent with accepted industry practices for emergency alerts.¹²⁵

42. There is broad support in the record for standardization of alert messages and adoption of the five recommended message elements. T-Mobile explains that the format "is designed to ensure that the most critical information is succinctly and clearly communicated in a manner most compatible with the technical attributes of wireless networks."¹²⁶ Purple Tree Technologies also supports the five message elements, but urges that event type and area affected be the only required elements, with others optional if space permits.¹²⁷ Based on our review of the record, we find that on balance the five message elements identified above will enable standardization of alerting messages and we hereby adopt them. We reject Alert Systems' claim that the element for "area affected" should be reconsidered, based on its hypothesis that "visitors and newcomers to areas often do not recognize geographic landmarks in warning messages."¹²⁸ A biohazard or flash flood warning, for example, would not enable the public to avoid a

¹²¹ WARN Act, § 602(b).

¹²² CMSAAC recommendations, § 5.3.1.

¹²³ *Id.*

¹²⁴ *Id.*

¹²⁵ *CMAS NPRM*, 22 FCC Rcd at 21981, ¶18.

¹²⁶ T-Mobile Comments at 18.

¹²⁷ Purple Tree Technologies Comments at 10.

¹²⁸ Alert Systems Comments at 16-17.

lethal hazard without appropriate area affected information. We also expect that as CMAS providers eventually deploy technologies capable of messages of more than 90 characters, additional alert message elements will be implemented.

43. In the *CMAS NPRM*, we also sought comment on whether alert messages should include telephone numbers, URLs¹²⁹ or other response and contact information, including any related network impacts.¹³⁰ The CMSAAC advised against inclusion of URLs or telephone numbers because such information would encourage mass access of wireless networks.¹³¹ The California Public Utility Commission (CAPUC) supports inclusion of a sixth message element for URLs, if feasible.¹³² AT&T (and many commenting parties) note that inclusion of a URL or telephone number in an emergency message, some of which might be delivered to tens of thousands of users in a matter of seconds, could lead to unacceptable network congestion and, in extreme cases, network failure.¹³³ We find that mandating URLs or telephone numbers in an emergency alert could exacerbate wireless network congestion at a time when network traffic is already dramatically increasing as individuals contact police, fire, and rescue personnel, as well as their loved ones.¹³⁴ We therefore will not require participating CMS providers to accept or transmit any alert message that contains an embedded URL or telephone number.

b. CMAS Generation of Free Text Alert Messages

44. In the *CMAS NPRM*, we sought comment on the CMSAAC's recommendation that the Alert Gateway automatically generate messages by extracting information from specified fields of a CAP-formatted message, SAME codes, or free-form text, which would then be transmitted across Reference Point C to electing CMS providers.¹³⁵ The CMSAAC recommended this approach for initial system deployments.¹³⁶ We also sought comment on the CMSAAC's recommendation to allow the generation of free text for Presidential and AMBER alert messages.¹³⁷ While numerous parties in this proceeding support adoption of the CMSAAC recommendations in full, few address the specific mechanics of generating alert messages via the Alert Gateway.¹³⁸ AT&T states that proposals for automatic generation of alert text "merit further investigation, but responsibility for the content of alerts should remain with initiators and the federal government—not wireless carriers."¹³⁹ We agree with AT&T and other parties

¹²⁹ URL is an acronym for Uniform Resource Locator and is a reference (an address) to a resource on the Internet. A URL has two main components: a protocol identifier and a resource name, which are separated by a colon and two forward slashes. The protocol identifier indicates the name of the protocol to be used to obtain the resource, such as HTTP (Hypertext Transfer Protocol). HTTP is just one of many protocols used to access different types of resources on the Internet. Other protocols include File Transfer Protocol (FTP), Gopher, File, and News. Additional information regarding URLs is available at <http://java.sun.com/docs/books/tutorial/networking/urls/index.html>.

¹³⁰ *CMAS NPRM*, 22 FCC Rcd at 21981-82, ¶20.

¹³¹ See CMSAAC recommendations, § 5.3.2.1.

¹³² See, e.g., CAPUC Comments at 12.

¹³³ AT&T Comments at 8; T-Mobile Comments at 19-20 (opposing inclusion of URLs, telephone numbers because "such information could cause customers to flood the wireless network resulting in crippling network congestion")

¹³⁴ See Alltel Reply Comments at 3 ("network congestion exists during emergencies today and would be made worse by inserting a phone number or URL to encourage people to initiate more calls"); RCA Reply Comments at 7 (inclusion of URLs or telephone numbers could make "it difficult or impossible for anyone to complete a critical telephone call" and possibly "tak[e] the entire wireless network down").

¹³⁵ *CMAS NPRM*, 22 FCC Rcd at 21981, ¶19; CMSAAC recommendations, § 5.3.2.

¹³⁶ See CMSAAC recommendations, § 5.3.2.

¹³⁷ *CMAS NPRM*, 22 FCC Rcd at 21981, ¶19; CMSAAC recommendations, § 5.3.3.

¹³⁸ See AAPC Comments at 5 ("urg[ing] the Commission to accept the recommendations as presented").

that electing CMS providers should act as a conduit for messages, the content of which is fixed before transmission to a CMS provider.

45. CellCast argues that we should “ignore” the CMSAAC recommendations regarding alert generation, asserting that message generation is beyond our mandate under the WARN Act.¹⁴⁰ The mechanisms for generating messages at the Alert Gateway are undefined currently and may be subject to implementation by the federal entity selected to administer the Alert Gateway. Nonetheless, we support the CMSAAC’s recommended approach of allowing the Alert Gateway to create messages using CAP fields and SAME codes.¹⁴¹ Specifically, we believe that this approach would enable the provision of consistent and accurate messages to the public, while facilitating future enhancements to the Alert Gateway.

46. We also agree with the CMSAAC that automatic generation of messages via CAP fields and SAME codes may not always provide sufficient flexibility to alert initiators to tailor messages for emergencies that may fall with the Imminent Threat Alert category.¹⁴² A message with a translated event code of “security warning,” for example, may not provide adequate information about a shooting incident on a college campus. A more apt warning might be “a shooting has occurred on the north campus,” with directions to “stay indoors.” We thus believe that the public interest would be served if the CMAS architecture accommodates free-form text messaging, subject to the 90-character text limit that we adopt today and our determination that electing CMS providers will generally not be obligated to accept or transmit any alert message that includes an embedded URL or phone number.¹⁴³ We also agree with the CMSAAC that free-form text should be included as a CAP message parameter.¹⁴⁴

47. Finally, we concur with the CMSAAC that automatic text generation at the Alert Gateway would be impractical for Presidential or AMBER Alerts,¹⁴⁵ both of which are likely to be highly fact specific. As the CMSAAC noted, the efficacy of a particular AMBER Alert hinges on specific information such as a description of a vehicle, abductor, or missing child.¹⁴⁶ Accordingly, we find that law enforcement authorities should have the ability to formulate unique message text for the dissemination of AMBER Alerts via the CMAS. We envision that such free text messages would be presented to the Alert Gateway in a free text CAP field. In the event of a Presidential Alert, we agree with the CMSSAC that, until such time as electing CMS providers are able to transmit messages longer than 90 characters, the Alert Gateway may employ a generic statement such as “The President has issued an emergency alert. Check local media for more details.”¹⁴⁷

4. Geo-targeting CMAS Alerts

48. The CMSAAC recommended that “to expedite initial deployments of CMAS an alert that is specified by a geocode, circle or polygon” should “be transmitted to an area not larger than the CMS

(...continued from previous page)

¹³⁹ AT&T Comments at 9.

¹⁴⁰ CellCast Comments at 36.

¹⁴¹ CMSAAC recommendations, § 5.3.2.

¹⁴² See CMSAAC recommendations, § 5.3.2.1.

¹⁴³ The only exception to this conclusion is the Presidential alert, which will be transmitted regardless of content provided it satisfies the 90 character limit.

¹⁴⁴ *Id.*

¹⁴⁵ CMSAAC recommendations, § 5.3.3.

¹⁴⁶ *Id.*

¹⁴⁷ *Id.*

[provider's] approximation of coverage for the county or counties with which that geocode, circle, or polygon intersects."¹⁴⁸ Based on the substantial record before us and for the reasons stated below, we require electing CMS providers to geographically target (geo-target) alerts accordingly. We note that radio frequency (RF) propagation areas for some paging systems and cell sites may exceed a single county, and we will permit geo-targeting that exceeds county boundaries in these limited circumstances.

49. Congress recognized the importance of geo-targeting alerts in the WARN Act. Specifically, in section 604 of the WARN Act, Congress directed the Under Secretary of Homeland Security for Science and Technology, in consultation with the National Institute of Standards and Technology (NIST) and the FCC, to establish a research program for "developing innovative technologies that will transmit geographically targeted emergency alerts to the public."¹⁴⁹ The Commission stands ready to work with DHS and NIST to facilitate this important undertaking.¹⁵⁰ We fully expect that as more refined and cost effective geo-targeting capabilities become available to electing CMS providers, they will voluntarily elect to target alerts more granularly. Several CMS providers have indicated their intention to geo-target alerts below the county level and we strongly encourage them to do so.¹⁵¹ As T-Mobile notes, electing CMS providers should be free to target more specifically, subject to the liability protections of the WARN Act.¹⁵²

50. In the *CMAS NPRM*, we sought comment on what level of precision the Commission should require for geo-targeting,¹⁵³ considering the CMSAAC's recommendation for county-level geo-targeting.¹⁵⁴ The CMSAAC recognized "that it is the goal of the CMAS for CMS providers to be able to deliver geo-targeted alerts to the areas specified by the Alert Initiator."¹⁵⁵ Based upon current capabilities and to expedite initial deployments, the CMSAAC recommended targeting "an area not larger than the CMS [provider's] approximation of coverage for the county or counties with which [a transmitted] geocode, circle, or polygon intersects."¹⁵⁶ The CMSAAC recommended that providers should be allowed (but not required) to deliver alerts to areas smaller than a county, using Geographic Names Identification System (GNIS) codes, polygon, or circle information to identify a predefined list of cell sites/paging transceivers within the alert area.¹⁵⁷

51. Several parties however urge us to mandate sub-county targeting. Alert Systems claims that disaster managers often require greater geographic granularity than that permitted by CAP and the CMSAAC recommendations.¹⁵⁸ Purple Tree Technologies asserts that sub-county targeting is "possible

¹⁴⁸ CMSAAC recommendations, § 5.4.

¹⁴⁹ WARN Act, § 604(b)(2).

¹⁵⁰ The CMSAAC recommends that we encourage DHS to establish a program under section 604 to develop geo-targeting technologies. CMSAAC Recommendations, § 5.4.

¹⁵¹ See, e.g., Alltel Comments at 4-5.

¹⁵² T-Mobile Comments at 17.

¹⁵³ *CMAS NPRM*, 22 FCC Rcd at 21982 ¶¶ 21-22.

¹⁵⁴ CMSAAC recommendations, § 5.4.

¹⁵⁵ *Id.* Systems used by Alert Initiators may allow them to define an alert area on a map. For example, the defined alert area could include the projected path of a tornado or an event that encompasses a portion of an urban area.

¹⁵⁶ *Id.* at § 5.4. The CMSAAC recommended that if a geocode, polygon, or circle is not transmitted with a non-presidential alert, the "Alert Gateway" should reject the message and return an error to the originator. *Id.* at App. B, § 10.3.2.22.

¹⁵⁷ CMSAAC Recommendations, § 10.3.2.

¹⁵⁸ Alert Systems Comments at 17, 18.

with cell broadcast,” and that there are few technical hurdles preventing granular alerts.¹⁵⁹ Acision and CellCast both contend that cell broadcast technology would allow for targeting to the individual cell level.¹⁶⁰ DataFM claims its technology could target “specific geographic areas without regard to the location of its transmitters.”¹⁶¹

52. The National Emergency Number Association (NENA) favors targeting smaller areas, noting that some counties are very large and that alert originators often need to target precisely.¹⁶² NENA asserts that targeting messages to the block level (similar to emergency telephone notification systems) would be “ideal,” but recognizes this is not possible.¹⁶³ The CAPUC argues that county targeting would be overbroad for most emergencies, and urges ZIP-code level targeting.¹⁶⁴ We note that there are more than 40,000 active ZIP codes in the United States, and many of these are assigned to specific addresses.¹⁶⁵ The CAPUC does not explain how ZIP code targeting could be implemented.¹⁶⁶

53. The weight of the record supports county-level targeting as recommended by the CMSAAC. CTIA, TIA and 3G Americas urge us to implement county-level targeting, with optional granularity, to encourage expeditious deployment of alerting capabilities.¹⁶⁷ T-Mobile agrees that electing CMS providers should not be not required to target alerts to areas smaller than a county, noting that given current technological limitations, many carriers would be unable to achieve more specificity.¹⁶⁸ Alltel also supports county-level targeting, but states that it intends to target more granularly.¹⁶⁹

54. MetroPCS notes that for smaller targeting areas, electing CMS providers would have to more precisely control the delivery of messages by the base stations serving a given targeted area than is currently economically feasible.¹⁷⁰ Similarly, The National Telecommunications Cooperative Association (NTCA) states that requiring electing rural CMS providers to send alerts to sub-county areas may be too expensive and may reduce the incentive to participate in the CMAS.¹⁷¹ The American Association of Paging Carriers (AAPC) opposes county-level targeting, noting that it may not be feasible for some

¹⁵⁹ Purple Tree Comments at 2, 11. We reject Purple Tree Technologies’ suggestion that polygon information should have priority over geocode information, which would be contrary to the CMSAAC Recommendations at § 5.3.1.

¹⁶⁰ Acision Comments at 6-7; CellCast Comments at 38-39. Westchester County, New York also supports the use of cell broadcast technology for sub-county targeting. *See* Westchester County Comments at 2, 3.

¹⁶¹ DataFM Comments at 12.

¹⁶² NENA Comments at 2.

¹⁶³ *Id.*

¹⁶⁴ CAPUC Comments at 13-15. *But see* NTCA Reply Comments at 4 (“The Commission should decline to follow the CAPUC’s suggestion and should, instead, adhere to the CMSAAC’s recommendation that emergency service alerts be geo-targeted and delivered no lower than the county-wide size area.”).

¹⁶⁵ *See* Census 2000 U.S. Gazetteer Files, available at <http://www.census.gov/geo/www/gazetteer/places2k.html>.

¹⁶⁶ We also note that New York City, which did not file comments, previously expressed concern that alerts should be targeted more precisely than county-level. *See CMAS NPRM*, 22 FCC Rcd at 21982, n.40.

¹⁶⁷ CTIA Comments at 7, 8; TIA Comments at 3, 4; 3G Americas Comments at 9.

¹⁶⁸ T-Mobile Comments at 17.

¹⁶⁹ Alltel Comments at 4-5.

¹⁷⁰ MetroPCS Comments at 4-5.

¹⁷¹ NTCA Reply Comments at 4.

paging providers to confine alerts to the county level, and that they would target alerts to the extent permitted by their networks.¹⁷²

55. Based on the foregoing, and subject to the limited exception discussed below, we conclude that it would be premature for us generally to require targeting of alerts more precisely than the county level. We specifically note that county-level targeting is consistent with the current practices of the National Weather Service, which is expected to originate many CMAS alerts. While some commenters argue that cell broadcast and perhaps other technologies could support more granular targeting,¹⁷³ the record indicates that not all CMS providers may employ cell broadcasting for their delivery of CMAS. Further, while several vendors urge us to mandate sub-county targeting,¹⁷⁴ at this point we find that the public interest is best served by enabling participating CMS providers to determine which technologies will most efficiently and cost effectively allow them to target alerts more precisely than the county level.

56. Accordingly, we generally require CMS providers that elect to participate in the CMAS to geographically target emergency alerts to the county level. In adopting this rule, we recognize the concerns of many CMS providers that face technical limitations on their ability to geo-target alerts to areas smaller than a county. In those limited circumstances where the propagation area of a paging system or cell site exceeds a single county, we will permit the RF signal carrying the alert to extend beyond a county's boundaries. Electing CMS providers may determine which network facilities, elements, and locations will be used to transmit alerts to mobile devices. Regarding the CMSAAC recommendation that, until such time as emergency alerts can be delivered to areas smaller than a county in real-time (*i.e.*, dynamic geo-targeting), certain urban areas with populations of greater than 1 million or with specialized alerting needs be identified for more precise geo-targeting,¹⁷⁵ we will address this recommendation once an entity has been identified to provide the Alert Aggregator and Gateway functions.

5. Meeting the Needs of Users, Including Individuals with Disabilities and the Elderly

57. Section 603(b)(3)(F) of the WARN Act required that the CMSAAC include representatives of national organizations representing people with special needs, including individuals with disabilities and the elderly.¹⁷⁶ Because the WARN Act directed the CMSAAC to submit recommendations to the Commission "as otherwise necessary to enable electing CMS providers to transmit emergency alerts to subscribers,"¹⁷⁷ the CMSAAC concluded, and we agree, that Congress intended to include the elderly and those with disabilities among the class to which electing CMS providers are to deliver alerts. Accordingly, we conclude that CMAS access to those with disabilities and the elderly falls within our obligation under section 602(a) of the WARN Act, and thus seek to ensure that commercial mobile alerts are accessible to all Americans, including individuals with disabilities and the elderly.

58. The CMSAAC recommended that the needs of individuals with disabilities and the elderly be addressed by, *inter alia*, the inclusion of a common audio attention signal, and a common

¹⁷² AAPC Comments at 7.

¹⁷³ See, e.g., Purple Tree Comments at 11, CAPUC Comments at 13-15, NENA Comments at 2, Alert Systems Comments at 17-18.

¹⁷⁴ See generally Acision Comments at 6-7; Alert Systems Comments at 17, 18; CellCast Comments at 38-39; DataFM Comments at 12; Purple Tree Comments at 2, 11.

¹⁷⁵ CMSAAC Recommendations, § 5.4.

¹⁷⁶ WARN Act, § 603(b)(3)(f).

¹⁷⁷ WARN Act, § 603(c)(7).

vibration cadence, on devices to be used for commercial mobile alerts.¹⁷⁸ The CMSAAC recommended that both functions be distinct from any other device alerts and restricted to use for commercial mobile alerting purposes.¹⁷⁹ The CMSAAC further noted that these features would benefit not only individuals with disabilities and the elderly, but also subscribers more generally.

59. For devices with polyphonic capabilities, the CMSAAC recommended that the audio attention signal should consist of more than one tone, in a frequency range below 2 kHz and preferably below 1 kHz, combined with an on-off pattern to make it easier for individuals with hearing loss to detect.¹⁸⁰ For devices with only a single frequency capability, the CMSAAC recommended an audio attention signal below 2 kHz.¹⁸¹ The CMSAAC also recommended that the unique vibration cadence should be noticeably different from the default cadence of the handset.¹⁸² The CMSAAC further recommended that if a device includes both the audio and vibration functions, simultaneous activation of both functions should not be required and that configuration should be determined by end users.¹⁸³

60. In the *CMAS NPRM*, we sought comment on the CMSAAC recommendations, including any technical or accessibility requirements that we should adopt to ensure that commercial mobile alerts will be received by individuals with disabilities and the elderly.¹⁸⁴ We asked whether attention signals should be required for all users.¹⁸⁵ We also noted that the CMSAAC recommended that alert initiators use clear and simple language whenever possible, with a minimal use of abbreviations and the ability to recall alert messages for review—and sought comment on these recommendations within the context of accessibility for individuals with disabilities and the elderly.¹⁸⁶

61. Nearly all commenting parties support the CMSAAC's recommendations for addressing the needs for individuals with disabilities and the elderly. AT&T, for example, states that adoption of the CMSAAC's recommendations for a common audio signal and vibration cadence will "allow for the immediate identification of emergency alerts" and foster "the widest possible distribution of alerts" to the public.¹⁸⁷ Alert Systems likewise notes that "[u]rgency coding of messages is vital,"¹⁸⁸ and that caretakers and operators of certain industrial facilities in particular "need unique alert tone patterns/amplitudes to quickly reprioritize activities."¹⁸⁹

62. The Wireless Rehabilitation Engineering Research Center for Wireless Technologies (Wireless RERC) supports adoption of a common audio attention signal, and recommends that we adopt the existing 8-second EAS attention signal for all users, asserting that it provides the necessary period of time to alert individuals with hearing disabilities.¹⁹⁰ The Wireless RERC also supports adoption of a

¹⁷⁸ CMSAAC recommendations, § 5.5.2.1.

¹⁷⁹ *Id.*

¹⁸⁰ *Id.*

¹⁸¹ *Id.*

¹⁸² *Id.*

¹⁸³ *Id.*

¹⁸⁴ *CMAS NPRM*, 22 FCC Rcd at 21982-83, ¶ 23.

¹⁸⁵ *Id.*

¹⁸⁶ *Id.*

¹⁸⁷ AT&T Comments at 15.

¹⁸⁸ Alert Systems Comments at 18.

¹⁸⁹ *Id.*

¹⁹⁰ Wireless RERC Comments at 11.

common vibration cadence, and states that electing CMS providers should provide clear instructions on the alert capabilities of their devices, including labels identifying mobile devices suitable for persons with audio and visual disabilities.¹⁹¹ AAPC supports the CMSAAC recommendations, but states that legacy devices should not be required to support such functions.¹⁹² CAPUC adds that although the CMSAAC was required to issue recommendations on wireless alerts exclusively, the Commission should consider ensuring interoperability with wireline devices for individuals with disabilities and the elderly, noting that some such users may not have access to wireless devices.¹⁹³ DataFM notes that it currently has equipment for text-to-speech for the blind and strobe light warnings for the deaf, and would employ audio alerts and vibration alerts for portable devices.¹⁹⁴

63. Although there is near unanimous support of the CMSAAC's recommendations for addressing the needs of individuals with disabilities and the elderly, several parties argue that no additional requirements are necessary. MetroPCS claims that the handsets that will be used to receive mobile alerts are already subject to disability access requirements, and any additional requirements may raise costs thereby discouraging CMS provider participation.¹⁹⁵ CellCast argues that no changes to CMS provider networks should be required, noting that some mobile devices can be configured to enable the elderly or blind to hear an audio conversion of the message using text-to-speech technologies.¹⁹⁶

64. We agree with the majority of those commenting and the CMSAAC that it is vital that we ensure access to commercial mobile alerts by individuals with disabilities and the elderly. We disagree with the premise articulated by some commenters that merely because some device manufacturers already include accessibility features for receipt of mobile alerts, no requirements are needed to ensure access to mobile alerts for individuals with disabilities and the elderly.

65. Accordingly, to address the needs of these user groups and the needs of users more generally, we will require that participating CMS providers include both a common vibration cadence and a common audio attention signal on any device offered to the public for reception of commercial mobile alerts.¹⁹⁷ Specifically, as the CMSAAC recommended, we specify a temporal pattern for the audio attention signal of one long tone of two (2) seconds, followed by two short tones of one (1) second each, with a half (0.5) second interval between the tones.¹⁹⁸ We will also require that the entire sequence be repeated twice with a half (0.5) second interval between repetitions.¹⁹⁹ For devices with polyphonic capabilities, we adopt the CMSAAC's recommendation that the audio attention signal consist of the two

¹⁹¹ *Id.* at 11-12. Wireless RERC also states that CMS providers should notify those subscribers whose mobile devices require upgrading to support CMAS. *Id.* at 12.

¹⁹² AAPC Comments at 7-8.

¹⁹³ *Id.* at 18.

¹⁹⁴ DataFM Comments at 12-13.

¹⁹⁵ MetroPCS Comments, *citing* 47 C.F.R. § 20.19.

¹⁹⁶ CellCast Comments at 43-44.

¹⁹⁷ The CMSAAC recommendations state that “[a] unique vibration cadence (if supported by the mobile device) should be provided as well as a unique audio attention signal.” CMSAAC Recommendations at § 5.5.2. To the extent that this language implies that CMAS-capable mobile devices do not have to supply a unique vibration cadence, we disagree. Rather, we believe that full access by people with hearing disabilities requires vibration capability. Given that most current mobile handsets are capable of programming dedicated audio and vibration ring tones, we do not believe that this requirement represents a significant burden for CMS providers or is inconsistent with the WARN Act.

¹⁹⁸ CMSAAC recommendations, § 7.2.

¹⁹⁹ *Id.*

EAS tones (853 Hz and 960 Hz). For devices with a monophonic capability, we will require that a universal audio attention signal be of 960 Hz (the higher frequency EAS tone).

66. We also seek to facilitate recognition of alerts for individuals that may have a hearing disability (or who may have muted the audio attention signal on their device), and therefore adopt the same temporal pattern for the vibration cadence as the CMSAAC recommended that the Commission specify for the audio attention signal. We strongly encourage CMS providers to coordinate with device manufacturers to utilize existing technologies to comply with these requirements as soon as possible.

67. We recognize that incorporating capabilities for a common audio attention signal and a common vibration cadence on the many devices that we expect to be offered to the public will take time to develop and implement successfully. However, we believe that assuring full access for all Americans is sufficiently important that equipment may not be considered CMAS compliant unless it includes both the common audio attention signal and the vibration cadence adopted in this Report and Order. Further, both functions must be distinct from any other incoming message alerts and restricted to use for CMAS alerting purposes. Finally, simultaneous activation of both the audio attention signal and vibration cadence is permissible.²⁰⁰

6. Output Mode/Display

68. The CMSAAC issued several recommendations regarding the output mode/display of mobile devices.²⁰¹ Specifically, the CMSAAC recommended that CMAS-enabled mobile devices should employ display fonts that are easily readable with recognizable characters, citing three typeface examples.²⁰² MetroPCS notes that certain accessibility requirements already apply to CMS providers, and that CMAS-enabled mobile devices will therefore accommodate certain disabilities.²⁰³ CellCast adds that the development of mobile devices is highly competitive and flexible enough to meet the needs of all users including those with special needs.²⁰⁴ Although we agree with the CMSAAC that “the goal in font selection is to use easily recognizable characters,”²⁰⁵ we do not want to constrain the ability of CMS providers and manufacturers of devices to implement display modes that they find will best meet the needs of people with disabilities and other users. Accordingly, we do not limit the display of CMAS alerts to a particular font or character set.

69. Text-to-speech (TTS) enabled wireless mobile devices are becoming increasingly common,²⁰⁶ and we strongly encourage all participating CMS providers to offer devices with such capabilities so that blind individuals and those with severe visual impairments can obtain the public safety benefits of commercial mobile alerts. We note that many of the requirements that we adopt today for the first generation of CMAS are intended to enable the provision of text-based alerts to the public. Although we envision that the CMAS will evolve to include audio and video service profiles, we find that at this initial stage of the CMAS, it would be premature to address the CMSAAC’s recommendations regarding output mode/displays for such future service profiles.

²⁰⁰ We agree with the CMSAAC that CMAS compliant mobile devices may include the capability to mute either or both of these features so that they will not be activated upon receipt of an alert. CMSAAC recommendations, § 7.3.

²⁰¹ See CMSAAC recommendations, § 5.5.2.3.

²⁰² *Id.*, citing Tips for Making Print More Readable, American Foundation for the Blind, available at <http://www.afb.org/Section.asp?SectionID=40&TopicID=200&DocumentID=210>.

²⁰³ MetroPCS Comments at 5, citing 47 C.F.R. § 20.19.

²⁰⁴ CellCast Comments at 43-44.

²⁰⁵ CMSAAC recommendations, § 5.5.2.3.

²⁰⁶ Information regarding TTS is <http://www.research.att.com/~ttsweb/tts/faq.php#TechWhat>.