Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of:	)	
	)	
Amendment of Part 11 of the Commission's	)	PS Docket No. 15-94
Rules Regarding the Emergency Alert System	)	
	)	
Wireless Emergency Alerts	)	PS Docket No. 15-91

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President and General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Matthew Gerst
Assistant Vice President, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

October 9, 2018

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of:	)	
	)	
Amendment of Part 11 of the Commission's	)	PS Docket No. 15-94
Rules Regarding the Emergency Alert System	)	
	)	
Wireless Emergency Alerts	)	PS Docket No. 15-91

COMMENTS OF CTIA

CTIA respectfully submits these reply comments in response to the Further Notice of Proposed Rulemaking seeking comment on proposals to facilitate false alert reporting and ensure that Wireless Emergency Alerts (WEA) are effectively delivered to the public.[1]

I. INTRODUCTION AND SUMMARY.

As CTIA and others explained in initial comments, the Wireless Emergency Alert system has become one of the most effective, efficient and reliable alert and warning tools for public safety and consumers across the country.[2] The WEA system's success is built on the forward-looking framework provided by Congress, the voluntary participation of wireless providers and support from device manufacturers, the unique partnership between the FCC, Federal Emergency Management Agency (FEMA), and the wireless industry, and a shared commitment to continued collaboration, assessment and enhancement of WEA.

CTIA explained in its initial comments, and the record confirms, that the Commission should proceed cautiously before taking steps to formalize its assessment of WEA performance and take care to avoid adopting performance requirements that would undermine the successful

[1] *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System; Wireless Emergency Alerts*, PS Docket Nos. 15-94, 15-91, FCC 18-94 (rel. July 13, 2018) (*WEA False Alert FNPRM*).

[2] Comments of CTIA, PS Docket Nos. 15-91, 15-94, at 1 (filed Sept. 10, 2018) (CTIA Comments).

WEA framework. As supported by the instant record, requiring Participating CMS Providers to track delivery or display of WEA messages would be infeasible without substantial changes to the foundational cell-broadcast technology used to meet the public safety mission of WEA. Moreover, any mandated performance requirements would undermine the voluntary nature of the WEA program as directed by Congress.

The record also makes clear that the Commission should proceed cautiously before considering proposals from commenters that would fundamentally restructure the successful WEA system. Proposals to utilize delivery confirmation technology or eliminate consumer "opt-out" choices not only implicate consumer privacy and choice over government-issued messages, but could further inhibit the ability of consumers and public safety personnel to communicate across commercial wireless networks after a WEA is sent. Instead, discussion among WEA stakeholders is necessary and appropriate to identify ways to achieve the goals of these commenters without undermining the WEA system. Further, the Commission should use this proceeding to encourage the industry and alert originators to collaboratively identify the root causes of non-delivery and non-display issues and identify effective methods to address any such issues.

In so doing, the Commission has the opportunity to draw on the successful delivery of more than 40,000 local and regional WEAs since 2012, and the first-ever nationwide Presidential Alert test message. Media outlets have reported that government officials estimated that 225 million wireless devices throughout the U.S. may have received FEMA's October 3rd, 2018 Presidential Alert test message.[3] Thus, FEMA's test of the Presidential Alert demonstrated that

[3] *See, e.g.*, Brian Fung, *Cellphone users nationwide just received a 'Presidential Alert.' Here's what to know*, WASHINGTON POST (Oct. 4, 2018), https://www.washingtonpost.com/technology/2018/10/03/millions-cellphone-users-are-about-get-

WEA remains one of the most effective and efficient ways to alert, warn, and inform wireless consumers in the U.S. within a matter of seconds.

As FEMA, the Commission, and WEA stakeholders evaluate the Presidential Alert and other recent test messages, CTIA supports Commission efforts to encourage all WEA stakeholders to work collaboratively in examining ways to further improve the delivery and display of WEA messages.

II. THE RECORD DEMONSTRATES THAT PERFORMANCE REQUIREMENTS WOULD INTERFERE WITH THE SUCCESSFUL WEA SYSTEM AND THAT WEA STAKEHOLDER COLLABORATION IS NECESSARY.

As CTIA explained in its initial comments, Participating CMS Providers serving 99 percent of wireless consumers and working collaboratively with equipment manufacturers, alert originators, and FEMA, have designed, implemented, and enhanced the WEA system to voluntarily distribute more than 40,000 WEA messages.[4] The success of the WEA system has been due in large part to the cell broadcast technology utilized for WEA messaging, which serves as an effective and efficient platform to deliver life-saving emergency messages to millions of wireless consumers without delays from network congestion on commercial channels.

CTIA agrees with commenters that highlight how WEA performance requirements that would impose specific delivery and reporting metrics on Participating CMS Providers not only would undermine the Congressionally-mandated voluntary nature of WEA, but also would require technical changes to the WEA system that may delay the delivery of critical, life-saving

---

presidential-alert-heres-what-know/?utm_term=.65744c66a95a ("Blasted out by cell towers nationwide over a 30-minute period, the message was expected to reach some 225 million people in an unprecedented federal exercise."); CBS This Morning, *Presidential Alert Works for Some, Not Others* (Oct. 4, 2018), https://www.cbsnews.com/video/presidential-alert-test-works-for-some-not-for-others/.

[4] Comments of CTIA, PS Docket Nos. 15-91, 15-94, at 1 (filed Sept. 10, 2018) (CTIA Comments).

information to wireless consumers. As AT&T notes, "[o]btaining accurate performance information, including delivery rates, presents challenges due to the one-way nature of the service."[5] Specifically, AT&T explains that "examining the reason for failure would require [it] to put the device in debug or logging mode—modes not currently enabled on consumer devices by device manufacturers—which, in isolation, makes it impossible for a network provider to identify the causes of any particular failure."[6]

While most wireless consumers receive WEA messages, the record documents several technical reasons that a WEA message may not be received or displayed. In the FNPRM, the Commission highlighted subscriber opt-out, device incompatibility, lack of radio coverage or device network connection, and use of a 3G device that is engaged in a voice or data session as reasons that a consumers may not receive a WEA message.[7] As CTIA further explained, subscribers with WEA-capable devices may also not receive WEA messages if their device is: (1) in Wi-Fi only mode; (2) served by a cell site that is outside the geo-targeted area for the alert, even though the device itself may be within the geo-targeted area; or (3) served by a network extender, repeater, or in-building microcell that is not identified by the Participating CMS Provider's network as part of an alert area.[8] AT&T also noted that a wireless subscriber may have an international device that does not conform to U.S. WEA standards, rendering it unable to

[5] Comments of AT&T, PS Docket Nos. 15-91, 15-94, at 2-3 (filed Sept. 10, 2018) (AT&T Comments).

[6] *Id.* at 3. *See also* Comments of Sean Donelan, PS Docket Nos. 15-91, 15-94, at 2 (filed Sept. 10, 2018) (noting that "hiding obscure debug data makes sense because most consumers have little use for the information under ordinary circumstances. Worse, the confusing WEA logs may prompt calls to carrier customer service centers [...] with questions about the debugging data.").

[7] *WEA False Alert FNPRM* ¶ 46.

[8] CTIA Comments at 5.

receive WEA messages.[9] Notably, imposing performance requirements on Participating CMS Providers would not change any of these technical factors.

CTIA agrees that a "holistic approach" among the WEA community, rather than defined performance metrics, is necessary to identify and resolve any message delivery issues.[10] Collaboration with FEMA, the FCC, and alert originator stakeholders could result in a successful approach that would provide necessary data to better assess WEA performance and identify root causes of any non-delivery or non-display issues.[11] Thus, imposing performance requirements on Participating CMS Providers would be premature before giving WEA stakeholders sufficient opportunities to work collaboratively to resolve any identified delivery or display issues.

III. PROPOSALS TO FUNDAMENTALLY CHANGE THE WEA SYSTEM REQUIRE FURTHER DISCUSSION ON WAYS TO UPHOLD CONSUMER PRIVACY AND CHOICE RELATED TO GOVERNMENT ISSUED MESSAGES.

Separate from the performance requirements proposed in the FNPRM, some alert originator commenters suggested that the Commission adopt proposals—such as imposing mandatory "read-receipt" capabilities or eliminating consumers' ability to opt out of non-Presidential alerts—that would further their public safety missions. However, such proposals would undermine the existing, successful WEA message delivery system by requiring fundamental changes that would implicate consumer privacy and run counter to the consumer choice that Congress intended. The Commission should instead encourage WEA stakeholders to work together to identify ways to further the public safety mission of alert originators, while maintaining consumer privacy and choice in government-issued WEA messages.

[9] AT&T Comments at 4.

[10] *Id.* at 5.

[11] CTIA Comments at 7.

For example, the New York City Emergency Management Department (NYCEM) encourages the Commission to evaluate whether to utilize "read-receipt-like" delivery confirmation technology for WEA messages. NYCEM argues that such an approach "limits the effort required on behalf of the WEA recipient, and leverages a capability that has long been included in consumer messaging technologies."[12] As NYCEM acknowledges, however, "most CMS providers have adopted broadcast technology for WEA delivery purposes and such technology is one-directional."[13] Thus, any requirement to utilize "read-receipt-like" technology would require a complete restructuring of the WEA system that would likely impact the ability of consumers and public safety personnel to communicate during an emergency by exacerbating congestion issues on commercial channels.

The use of "read-receipt-like" technology also would raise privacy concerns from consumers that the Commission would have to thoroughly address before considering this proposal. While some media reports noted that "[t]he FCC has a pretty helpful FAQ that explains, among other things, that, no, you can't be tracked via this system . . . ," significant public concern was expressed about the perceived privacy implications of WEA prior to FEMA's recent Presidential Alert test message.[14] Indeed, Jeramie Scott, director of the

[12] Comments of the New York City Emergency Management Department, PS Docket Nos. 15-91, 15-94, at 4 (filed Sept. 10, 2018) (NYCEM Comments).

[13] *Id.*

[14] *See* Marcus Gilmer, *FEMA to test a new system that allows the president to send an alert to your phone*, MASHABLE (Sept. 15, 2018), https://mashable.com/article/trump-emergency-alert-text-message/#ayrJaTaScgql. *See also* Emily Stewart, *FEMA is testing a new "presidential alerts" system that sends messages to your phone*, VOX (Sept. 15, 2018), https://www.vox.com/policy-and-politics/2018/9/15/17863954/presidential-alert-trump-fema-emergency-alert-test; Farnoush Amiri, *Trump can't use FEMA's wireless alerts to send personal messages—it's illegal*, NBC NEWS (Sept. 18, 2018), https://www.nbcnews.com/tech/tech-news/trump-can-t-use-fema-s-wireless-alerts-send-personal-n910676.

Electronic Privacy Information Center's Domestic Surveillance Project, said that without more information on the breadth and reach of the WEA system, there could be a risk of abuse due to its "intrusive" nature.[15] Thus, if the Commission were to even consider technology that would indicate when a subscriber has or has not received or read a specific WEA message, the Commission should thoroughly consider potential privacy concerns consumers may raise about alert originators collecting and acting upon such information.

The Commission should also consider whether "read-receipt-like" technology would inhibit consumer communications during an emergency due to the exacerbation of network congestion issues on commercial channels.[16] For example, for the three million-plus mobile wireless subscribers in the Washington DC Metro area, a Participating CMS Provider's network would not only have to disseminate the WEA messages to these subscribers, but also manage traffic created by more than three million wireless subscribers' simultaneous return messages indicating that the message has been delivered, followed by confirmations that the message has been read. Doing so would likely create network performance issues that could impair the ability of wireless subscribers, and potentially public safety personnel, to communicate in times of emergency.

---

[15] *See* Farnoush Amiri, *FEMA's 'Presidential Alert' test postponed as some Americans want to disconnect*, NBC NEWS (Sept. 17, 2018), https://www.nbcnews.com/tech/mobile/fema-s-presidential-alert-test-postponed-some-americans-want-disconnect-n910406.

[16] This type of network congestion is substantially different than the type that may be created from clicking an embedded reference (or URL) within a WEA message. *See e.g.*¸ CTIA Petition for Reconsideration, PS Docket Nos. 15-91 and 15-94, at 2 (filed Dec. 1, 2016). In that case, a subscriber must take an action (clicking the link) to initiate communications on the network. Here, a read receipt would occur without any affirmative action by a consumer—ensuring that there will be more data traffic and providing no "opt out" alternative if the user has no ability to not provide this information.

Despite all of these concerns, CTIA and its member companies appreciate the goal of NYCEM to enhance WEA and further their public safety mission. Rather than moving forward on this proposal, however, the Commission should encourage WEA stakeholders to work together to consider ways to achieve NYCEM's goals in ways that uphold consumer privacy and mitigate network congestion issues.

Additionally, Harris County's suggestion to remove consumer choice to "opt-out" of non-Presidential Alert WEA messages is something that only Congress should consider.[17] Under Section 602(b)(2)(E) of the Warning, Alert, and Response Network Act (WARN Act), Participating CMS Providers "may offer subscribers the capability of preventing the subscriber's device from receiving such alerts, or classes of such alerts, other than an alert issues by the President."[18] Thus, Congress clearly directed the Commission and participating CMS providers to allow consumers to choose to "opt-out" of receiving certain WEA messages. In addition, the Commission noted that the WARN Act "authorizes participating CMS providers to allow device users to prevent the receipt of alerts or class of alerts" other than Presidential alerts.[19]

Congress and the Commission's recognition of the importance of consumer choice over a decade ago has been recently supported by initial reactions to FEMA's recent non-opt-out Presidential Alert test message. For example, many subscribers expressed concerns about the mandatory nature of Presidential Alerts.[20] Given the importance of consumer choice in WEA,

---

[17] Comments of Harris County, Texas, PS Docket Nos. 15-91, 15-94, at 2 (filed Sept. 10, 2018).

[18] 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, § 602(b)(2)(E) (2006) (WARN Act).

[19] *See Commercial Mobile Alert System*, First Report and Order, 23 FCC Rcd 6144, 6156 ¶ 28 (2008).

[20] *See* Farnoush Amiri, *FEMA's 'Presidential Alert' test postponed as some Americans want to disconnect*, NBC NEWS (Sept. 17, 2018), https://www.nbcnews.com/tech/mobile/fema-s-presidential-alert-test-postponed-some-americans-want-disconnect-n910406; Chris Riotta, *Presidential alert text messages arriving Wednesday after fierce pushback*, THE INDEPENDENT (Oct. 1, 2018),

the Commission should appropriately defer to Congress on the question of whether the receipt of any WEA messages beyond Presidential Alerts should be mandatory.

IV. THE WEA SYSTEM HAS SUCCESSFULLY USED BUILT-IN REDUNDANCIES TO SEND THOUSANDS OF WEA MESSAGES.

Despite the overwhelming success of the existing WEA program, the Public Television Broadcasters urge the Commission to establish rules that require use of the public television Warning, Alert, and Response Network (WARN) system as a redundant alternate delivery mechanism for alert messages between IPAWS and Participating CMS Providers.[21] While Section 602(c) of the WARN Act requires broadcast licensees, noncommercial educational broadcast stations, and public broadcast stations to install such equipment "to enable the distribution of geographically targeted alerts" by Participating CMS Providers,[22] Congress did not mandate that that this equipment or technology be utilized as a redundant pathway. This is underscored by the Commission's implementation of Section 602(c), in which it noted that the equipment and technology installed would "provide participating CMS providers with a redundant, alternate distribution path *by which they may choose* to receive geo-targeted CMAS alerts from the Alert Gateway."[23]

---

https://www.independent.co.uk/news/world/americas/text-alert-president-donald-trump-emergency-message-phones-when-what-a8564151.html; Josh Gerstein, *Suit seeks to block Trump from sending 'presidential alerts' to phones*, POLITICO (Oct. 1, 2018), https://www.politico.com/story/2018/10/01/trump-presidential-alerts-to-phones-857287. *See also* Beth Skwarecki, *How to Avoid an 'Unblockable' Presidential Alert*, LIFEHACKER (Sept. 18, 2018).

[21] Comments of America's Public Television Stations, the Corporation for Public Broadcasting, and the Public Broadcasting Service, PS Docket Nos. 15-91, 15-94, at 2-3 (filed Sept. 10, 2018).

[22] *See* WARN Act § 602(c).

[23] *Commercial Mobile Alert System*, Second Report and Order and Further Notice of Proposed Rulemaking, 23 FCC Rcd 10765, 10771 ¶ 16 (2008).

In fact, redundancies have been built into the standards developed for the WEA system since its inception that renders additional, mandated redundancies unnecessary.[24] Specifically, the WEA system was designed to adhere to the "trust model" recommended by the Commission's Commercial Mobile Service Alert Advisory Committee (CMSAAC). The CMSAAC recommended that IPAWS "be protected against the potential for misuse such as hoax emergency alerts, illegal distribution of offensive content, Denial of Service (DoS/DDoS) attacks and SPAM" in part by being "geographically redundant" to avoid a single point of failure.[25] CMSAAC also recommended that the Commercial Mobile Service Provider Gateway "have redundancy and be designed to provide high reliability and availability comparable to similarly situation network elements."[26]

Participating CMS Providers and FEMA carried out these recommendations and spent considerable time and effort designing a highly reliable, redundant, and secure interface to deliver WEA messages. To the extent a redundant path between IPAWS and Participating CMS providers' gateways are necessary, the FCC's Communications Security, Reliability and Interoperability Council (CSRIC) has noted that FEMA should take steps to ensure the security and reliability of IPAWS.[27] There is therefore no need for the Commission to consider mandating that participating CMS providers utilize public television's WARN system as a redundant alternate delivery mechanism for alerts from IPAWS when the existing WEA system

[24] *See e.g.*, ATIS J-STD-101.

[25] *See Commercial Mobile Alert System*, Notice of Proposed Rulemaking, 22 FCC Rcd 21975, 22018, 22079 (2007).

[26] *Id.* at 22020.

[27] Communications Security, Reliability and Interoperability Council V (CSRIC V), Working Group 2 – Emergency Alerting Platforms, WEA Security Sub-Working Group (WG-2), *Final Report – WEA Security*, at 29-30 (Mar. 2016), https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG2_WEA-Sec-Sub_FinalReport_0316.docx.

has successfully delivered more than 40,000 WEA messages to wireless consumers without such a requirement.

V. CONCLUSION.

CTIA and its member companies support the Commission's efforts to ensure that wireless consumers continue to be reliably served by the WEA system. With that in mind, however, it is critical that the Commission not impose requirements that could have unintended consequences for the delivery of critical, potentially life-saving information. Instead of mandating specific performance or reporting requirements, CTIA supports Commission efforts to encourage all WEA stakeholders to work collaboratively to examine how the all parties can further improve the delivery and display of WEA messages.

Respectfully Submitted,

/s/ Matthew Gerst

Matthew Gerst
Assistant Vice President, Regulatory Affairs

Thomas C. Power
Senior Vice President and General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

Dated: October 9, 2018