

TABLE OF CONTENTS

	Page
I. Introduction and Summary	1
II. Enhancements Intended to Improve the Effectiveness of WEA Message Content	5
A. Increasing Maximum WEA Character Length.....	5
B. Coexistence of 90 and 360-Character Messages.....	6
C. Costs Associated with the Change to Longer WEA Messages	9
D. Creation of the Category “Emergency Government Information”	10
E. Content in WEA Alerts	13
F. Multilingual WEA messages.....	17
III. WEA Geo-Targeting.....	18
IV. Alert Logging and Test Reporting	20
V. Provisions Affecting Participating CMS Providers and Subscribers.....	23
CONCLUSION.....	24
APPENDIX 1.....	25
APPENDIX 2.....	27

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

In the Matter of)
Improving Wireless Emergency Alerts and) PS Docket No. 15-91
Community-Initiated Alerting)

COMMENTS OF AT&T

AT&T Services Inc. (“AT&T”) hereby submits the following comments in response to the Federal Communications Commission’s (“Commission”) Notice of Proposed Rulemaking (“Notice”) in the proceeding captioned above.¹ In the Notice, the Commission proposed several enhancements to the existing Wireless Emergency Alert (“WEA”) system. AT&T supports some of those proposed enhancements; however, as seen below, it disagrees with other of the Notice’s proposals.

I. Introduction and Summary

In choosing among the proposals presented in the Notice, AT&T has sought to keep in mind the purpose for which Congress created WEA.² WEA is not meant to be a full source of information in an emergency;³ it is but one of several information pathways, which include tradi-

¹ See, Notice of Proposed Rulemaking, PS Docket No. 15-91, FCC 15-154 (November 19, 2015).

² The NAS shall “alert the public to any imminent threat that presents a significant risk of injury or death to the public...” *Warning, Alert, and Response Network Act (“WARN Act”)*, Pub. L. No. 109-347, §603(a) (2006) at Section 2(b).

³ Executive Order 13407 called for a “secure delivery of coordinated messages to the American people through as many communication pathways as practicable...” Executive Order 13407—Public Alert and Warning System (June 26, 2006) at Section (2)(a)(i). See also, *WARN Act*, Pub. L. No. 109-347, §603(a) (2006) at Section 2(b)(4).

[NAS] will transmit alerts across the greatest possible variety of communications technologies, including digital and analog broadcasts, cable and satellite television, satellite and terrestrial radio, wireless communications, wireline communications, and the Internet to reach the largest portion of the affected population.

tional EAS via AM, FM, and TV broadcast stations, cable systems, wireline video systems, wireless cable systems, Direct Broadcast Satellite (DBS) services, Satellite Digital Audio Radio Service (SDARS), as well as other participating entities like NOAA Weather Radio. WEA complements these dissemination methods by providing a concise, geographically targeted message. WEA should remain a “bell ringer” service, as intended by Congress, designed to get the public’s attention and to provide immediate instructions to people in the affected area. After receiving a WEA, members of the public can turn to other information sources, like broadcast radio, television, or the Internet for more detailed information.

One of WEA’s challenges is to inform the recipients to “check local media” for further information. In many cases, the local media are not carrying the emergency alert or providing further instructions to the recipients who tune in to seek that information. WEA, by its short-message nature, cannot effectively close this information gap by new rules changing it from a bell ringer service into a full media information source. The FCC should not attempt to compensate for the under-participation of the other members in the EAS by overburdening WEA. Instead, AT&T believes the Commission should consider amending its rules for EAS to require that when a WEA message is generated from an alert originator, an EAS message is also disseminated by all available public warning systems to provide additional information on the alert.

With these points in mind, AT&T supports the Notice’s proposal to increase WEA message length to 360 characters for 4G capable devices while maintaining the existing 90-character messages for 2G and 3G devices. However, the company opposes increasing WEA message length beyond 360 characters for several reasons, not the least of which is the effect of increased message length on delivery times for alerts and the possibility of confusing alert recipients with lengthy messages. AT&T also supports the creation of the Emergency Government Information category;

as explained more fully below, the company urges the FCC to continue to require alert generators to be vetted and trained by FEMA. AT&T views this as critical to protecting the security and integrity of the WEA system.

The Notice also asks about the advisability of transmitting alerts in multiple languages. Aside from Spanish, AT&T regards alert transmission in multiple languages as impracticable because of the increased burden it would place on the cell broadcast network, upon which WEA depends for its operation.

AT&T supports the Notice's proposal for alert logging and test reporting.

As noted, AT&T cannot support all of the proposals in the Notice. For example, the company opposes the Commission's proposal to remove Section 10.440 from its Part 10 WEA rules to allow embedded phone numbers and URLs to be included in WEA messages. AT&T agrees with the findings of studies concluding that URLs and telephone numbers in WEA alerts will lead to network congestion. The Notice suggests the inclusion of multimedia content or graphic content like maps in the WEA alerts. This suggestion is not feasible because multimedia is not supported by existing cell broadcast technology. Full multimedia content requires new technologies whose deployment will be driven by commercial demand; consequently, multimedia coverage will lag behind WEA coverage.

The Notice proposes to revise the Commission's rules to require that Participating CMS Providers must transmit any alert message that is specified by a geocode, circle, or polygon to a target area not larger than the specified geocode, circle, or polygon. AT&T does not support this proposal because specifying the target area to be "not larger" than the alert area may actually produce a significant "undershoot" of the alert polygon and force the transmitting entity to exclude

cell sites on the polygon border, or even just outside the polygon, to get the best approximation of that polygon.

II. Enhancements Intended to Improve the Effectiveness of WEA Message Content

A. Increasing Maximum WEA Character Length

AT&T supports increasing the maximum number of characters in a WEA message from 90 to 360 on 4G LTE networks, while maintaining the current 90-character limit for 2G and 3G devices as the Commission proposes.⁴

As WEA messages become longer, the possibility of longer delivery times increases. The use of 360 characters as described in the ATIS (Alliance for Telecommunications Industry Solutions) Feasibility Study is a compromise solution that delivers a longer message to the user without adding significant delays in its delivery.⁵ Nonetheless, some entities have suggested increasing the maximum WEA character length to as much as 1,380 characters⁶ in the apparent belief that longer WEA messages would be more effective at guiding people to take protective action. AT&T does not agree that WEA messages longer than 360 characters would serve the public interest during life-threatening emergencies.

Lapidary expression is not an attribute of government.⁷ Inevitably, WEA messages will expand to use whatever number of characters are available to them, just as work expands to fill the time available for its completion.⁸ Such a lengthening of messages will prove as useful to WEA as the expansion of work is to productivity. Prolixity offers no better service to the person facing

⁴ Notice at ¶ 9.

⁵ ATIS Feasibility Study for LTE WEA Message Length (“ATIS Study”) at 12. https://access.atis.org/apps/group_public/download.php/25045/ATIS-0700023.pdf

⁶ *See, e.g.*, DEPARTMENT OF HOMELAND SECURITY STUDY OF TERRORISM AND RESPONSES TO TERRORISM, COMPREHENSIVE TESTING OF IMMINENT THREAT PUBLIC MESSAGES FOR MOBILE DEVICES 37 (2014) (START Report) at 30.

⁷ “The Lord’s Prayer is 66 words, the Gettysburg Address is 286 words, there are 1,322 words in the Declaration of Independence, but government regulations on the sale of cabbage total 26,911 words.” David McIntoshin

⁸ C. Northcote Parkinson, *Parkinson’s Law: The Pursuit of Progress* (London, John Murray, 1958).

a life-threatening emergency than does conciseness; indeed, such messages may actually harm the public.⁹ ATIS noted in its study¹⁰ of WEA message length that broadcast of such long messages may delay receipt of the message, or be difficult to read and comprehend on small-screen mobile devices. Moreover, subscribers with low-end feature phones could have difficulty receiving and comprehending such messages.

It may be that studies are needed to determine the character length that best supports the “bell ringer” purpose of WEA. However, from a rulemaking view, AT&T supports an increase of WEA message length of up to 360 characters, while letting policy and best practices, along with studies, determine the proper character length (up to 360) that alert originators should use in a given circumstance. The goal should be to make WEA service easy to use in the support of public safety and not to give users reasons to opt out because of confusing messages. Furthermore, with the standards for 5G now under development, it is important to have agreement that a WEA message length of 360 characters is the maximum length for 4G and future services.

B. Coexistence of 90 and 360-Character Messages

The Notice seeks comment on the view that the existing 90-character limit should remain for legacy networks and devices because of these networks’ limitations and the expectation that the overwhelming majority of Commercial Mobile Service Provider (CMSP) infrastructure and mobile devices will soon achieve 4G LTE capability. AT&T supports this view.

For some time to come, 2G and 3G networks will continue to exist in the United States. These networks, as the Commission recognized,¹¹ cannot receive 360-character WEA messages.

⁹ For example, subscribers who are driving may be distracted by these lengthy messages.

¹⁰ ATIS Study at 12 *et seq.*

¹¹ Notice at ¶9.

In order to support 360 characters on the 4G and future networks, alert originators must provide CMSPs with both the 90-character and 360-character message.

Alert originators have a couple of ways to provide alerts that will meet the 90 and 360-character burden. For example, it is possible for alert originators to create only one message; the first 90 characters of such a message would contain the essential information (What’s Happening, Area Affected, Recommended Action, Expiration Time, and Sending Agency) defined by the Commercial Mobile Service Alert Advisory Committee (“CMSAAC”),¹² and the remaining characters (up to the 360 limit) would provide expanded information that capable 4G devices can receive and display.¹³ Another approach would be for the alert originator to create two WEA alert messages, the first adhering to the 90 displayable character maximum and the second to support the 360 displayable character length

Another suggestion has been made that the transmission of a 360-character message may be made in four parts of 90-characters each over legacy networks (and in a single message over 4G networks, where feasible).¹⁴ This solution is not feasible for 2G and 3G Networks. In these legacy networks, there is no guarantee of message receipt or (more to the point for those who prize clarity in their emergency communications) of receiving the four message parts in the proper order. Legacy devices would not be able to correlate the four segments of the message and put them together into one coherent message – it would have to be left to the user to rely upon his memory, at a time when he is bombarded by sensation, to reconstruct the overall message by recalling the

¹² Commercial Mobile Service Alert Advisory Committee, Commercial Mobile Alert Service Architecture and Requirements (“CMSAAC Report”) at § 5.3.1. See, *In the Matter of The Commercial Mobile Alert System*, PS Docket No.07-287, Notice of Proposed Rulemaking (December 14, 2007), Appendix B.

¹³ The splitting of the message into a 90-character message and 360-character message must be a FEMA IPAWS function, as the CMSPs do “not manipulate messages” and do not want the responsibility for making certain that someone else’s message is properly “split”.

¹⁴ Notice at ¶ 14.

four parts and putting them in the proper order if they were all received. Obviously, a regulatory wager that a subscriber could do this in the midst of an emergency is not worth taking.

Support for both 90 and 360-character messages will require changes to the interface between the FEMA IPAWS (“Integrated Public Alert and Warning System”) and the CMSP network,¹⁵ and changes to the CMSP infrastructure. The changes will first require modifications to industry standards,¹⁶ followed by development, testing, and deployment of the changes. While this requires technical changes with associated costs, they are feasible so long as the timelines in which to complete these activities are realistic. Standards changes alone will require a minimum of 12 months, followed by changes to the CMSP infrastructure, including development, testing and deployment. Coordination with changes to the FEMA IPAWS is required, as well as with alert originator updates. One year is not feasible for such changes, and AT&T estimates that it would take 24-30 months, rather than just one year, to perform all of the tasks required to achieve compliance. In addition, any such changes in the CMSP network without associated changes on the alert originator side will remain useless until alert originators can provide both the 90 and 360-character messages.

As long as there are 2G and 3G networks deployed in the U.S., alert originators will need to deal with the co-existence issues between the 90-character and 360-character messages. While operators are deploying 4G LTE nationwide, there remain areas of coverage with only 3G (and even 2G) systems. In order to get the WEA message out to the maximum number of citizens, support for those legacy networks must remain until there are no functional 2G or 3G networks deployed.

¹⁵ CMSAAC and industry standards define this as the C interface.

¹⁶ *See*, Appendix 1 for a list of existing standards that would require change to accommodate the coexistence of the 90 and 360-character messages.

C. Costs Associated with the Change to Longer WEA Messages

WEA is a purpose-built system that leverages and runs on top of the standards-defined cell broadcast service. While much of the underlying technology is designed to support commercial cell broadcast services, certain elements in the WEA infrastructure are WEA specific, most notably the CMSP Gateway as defined in the CMSAAC Report.¹⁷ Any cost for modifications to increase the maximum character length is mainly contained to the WEA-specific CMSP infrastructure and does not affect the underlying cell broadcast technology; these are costs that the CMSP must absorb to continue to meet its obligations as a Participating CMSP.

Plainly, infrastructure exists to support 90-character messages. Adding a 360-character message to the 90-character message does not affect the underlying cell broadcast technology, but does affect the CMSP Gateway and interface to the FEMA IPAWS. AT&T believes that the co-existence of 90 characters for legacy and 360 characters for 4G LTE balances the burden and obligation on the participating CMSP with the desires of the alerting community at a reasonable cost.

Still, AT&T has expressed concerns that enhancements to WEA beyond the original CMSAAC-proposed design will impose costs upon CMSPs that small and rural carriers may not be able to bear. This is especially true for some of the changes proposed in this NPRM that go beyond simply increasing message length. In order to keep WEA viable for all stakeholders, the design and proposed enhancements must be thoroughly vetted, with particular attention to the cost of implementation and operation. WEA should be viewed as one component in an overall alerting system, and CMSPs should not bear the burden of trying to design their networks to be a purpose-

¹⁷ CMSAAC Report at § 2.2.4.

built alerting platform. In this way, WEA will continue to remain a viable “bell ringer” solution in an overall alerting policy.

D. Creation of the Category “Emergency Government Information”

The Commission proposes to create a new WEA category called Emergency Government Information, and asks whether enabling the delivery of Emergency Government Information messages would expand the alerting means available to government entities in a meaningful way, complementing existing WEA classes and allowing the provision of more detailed information about how to protect life and property. AT&T supports the creation of this new category.

Emergency Government Information should be a standalone message generated from credentialed, authorized, and trained alert originators, but directly related to a WEA Alert. Because emergencies are local, it should be left to the local emergency management authorities to determine whether an “Emergency Government Information” is related to an imminent threat to life and property. Trying to codify a strict definition will only serve to limit the effectiveness of this tool. There should be no conditions set in FCC rules, or in FEMA policy. That said, best practices should be developed with guidelines on what constitutes an Emergency Government Information message and how it relates to an imminent threat.

Only the set of alert originators authorized to send out WEA Alerts should be permitted to generate Emergency Government Information (“EGI”) messages. Today, this set of alert originators are vetted, credentialed, and trained by FEMA. This differentiates WEA from other “mass notification systems” where there is no such credentialing or vetting of those who may issue an alert. Given that improper use of this new category raises concern about consumer dissatisfaction with WEA and subsequent opt-outs from it, training of local alerting authorities is essential for all alert messaging over WEA. FEMA and alert originators should develop “best practices” for WEA

alert creation, including use of EGI. By maintaining consistency in vetting alert originators, the security risk is reduced and the integrity of the WEA system is better assured.

The introduction of the new WEA category must be done carefully to avoid customer confusion and compatibility problems with existing, deployed devices. Proprietary solutions, which are inconsistent with this goal and work against the purpose of WEA, should be forbidden. This will prevent public confusion about WEA operations across devices or service providers. Any change to WEA must be standardized to assure facile and effortless access across devices and CMSPs.

Depending on whether EGI is part of an existing opt-out option (*i.e.*, lumped together with Amber Alerts or Imminent Threat Alerts) or as a new opt-out category¹⁸ will dictate the level of standards changes, CMSP infrastructure changes, and mobile device changes required. The FCC Rules should not dictate the implementation, but leave it to standards bodies to study and define the appropriate solution.¹⁹

AT&T regards EGI as an adjunct of imminent threat alerts and is intended to provide the public with important information related to an imminent threat. The use of EGI needs to be monitored and policed by FEMA to prevent confusion and over-use. AT&T opposes the creation of additional WEA categories beyond Essential Government Information because additional WEA categories beyond EGI will have enormous backward compatibility issues with deployed handsets,

¹⁸ The Notice asks if it would be preferable for Emergency Government Information to be presented to consumers on an opt-in basis. Notice at ¶ 21. In AT&T's view, an "opt-in" solution is not permitted for any WEA category. Any commercial mobile service licensee electing to transmit emergency alerts may offer subscribers the capability of preventing the subscriber's device from receiving such alerts, or classes of such alerts, other than an alert issued by the President.

WARN Act at Section 3(d)(2)(E).

¹⁹ See, Appendix 2 for the standards changes to support the creation of a new category requiring a new opt-out entry on the device menu.

and cause unnecessary and costly changes to the CMSP infrastructure. It will cause public confusion (especially with multiple “attention signals”). WEA has a specific, defined task– to provide presidential, imminent threat, and Amber alerts. While AT&T has agreed to add Emergency Government Information as an adjunct of imminent threat alerts, we must keep in mind that WEA is a complimentary service to private mass notification systems and has a more direct purpose of alerting the public to any imminent threat that presents a significant risk of injury or death to the public;²⁰ thus, WEA should not support additional alert types. Given WEA is available on a significant majority of mobile devices, adding additional categories will only serve to dissuade the public from keeping the service enabled as they become deluged with alerts that do not bear directly on their lives or property. Indeed, there is on-going concern that the WEA will fall victim to the “car alarm” syndrome, and adding additional categories will only heighten that concern.

As noted above, WEA alert originators are vetted, credentialed and trained as part of FEMA’s IPAWS process. Mass Notifications Systems, which go well beyond local governments and into private schools, universities, and businesses, can affect the security and integrity of the WEA system. Local jurisdictions should be urged to use WEA instead of these mass notification systems for imminent threat alerts in their communities, reserving mass notification systems and cell broadcast-based systems for notification services outside of WEA.

Other mass notification services, such as those used for general information or non-imminent threat messages, should not become a part of WEA. This will only discredit the WEA system, result in more harm than good, potentially causing more consumers to opt-out of WEA. In addition, FEMA would lose control of the vetting and credentialing of the mass notification originators,

²⁰ *See*, n. 2 above.

resulting in a significant increase in security risk to the “core” WEA system. Instead, mass notification systems should explore other options available using commercial cell broadcast services.

WEA should hew tightly to its congressionally defined purpose and maintain the strict definition of serving the public in times of imminent threat to life or property. AT&T believes the WEA messages should be driven by the local authorities, who are in the best position to determine what messaging their constituents need in times of emergency. WEA technology must not bear the burden of every alert category; it must adhere to its core mission.

E. Content in WEA Alerts

AT&T opposes the Commission’s proposal to remove Section 10.440 from its Part 10 WEA rules, to allow embedded phone numbers and URLs to be included in WEA messages.²¹

AT&T agrees with the conclusions of the ATIS Study that URLs and telephone numbers should not be contained in WEA Alerts.²² The ATIS Feasibility Study addresses CSRIC²³ IV, START and FEMA’s recommendation of further study on whether the inclusion of URLs in WEA messages could cause network congestion when many people try to gain access to a link within seconds of an alert. ATIS concluded that introducing URLs in a WEA message will result in significant challenges within the CMSP infrastructure network, including network congestion to the point of blocking communications.²⁴

²¹ Notice at ¶ 25.

²² FEASIBILITY STUDY FOR WEA SUPPLEMENTAL TEXT (“Supplemental Study”) at § 5.5. https://access.atis.org/apps/group_public/download.php/25923/ATIS-0700026_WEA_Supplemental.pdf

²³ The Communications Security, Reliability and Interoperability Council

²⁴ ATIS also noted that there are cybersecurity issues associated with vulnerable websites and disadvantages to citizens who have Internet access restrictions that could make the retrieval of additional WEA alert information through URLs difficult or altogether impossible. Supplemental Study at § 5.5.

The fundamental principles of cellular systems have not changed since the CMSAAC report concluded that a telephone number or URL in a WEA message would encourage mass attempts to log onto wireless networks, thereby creating congestion in the midst of an emergency.²⁵ A cellular system is a shared resource limited contention-based system. The wireless network itself is engineered to serve voice and data traffic use anticipated during peak usage, the “busy hour.” There are limits to the number of simultaneous voice or data connections that any CMSP has available. In everyday scenarios, wireless networks are challenged to keep up with the exploding demand for service; they do so with deployments of small cells, Wi-Fi off-loading, and other technologies. Carriers can react to anticipated spikes in demand by adding temporary sites to boost capacity, such as for the Super Bowl, thereby reducing the potential for slower data speeds and blockage. By contrast, when a disaster strikes, networks are stressed beyond their limits because the need for voice and data services grossly exceeds normal, everyday use. Anyone who has had the misfortune to experience such an event knows that even robust networks often cannot meet the incessant demands for both voice and data service. This includes critical communications to 911 (police/fire/EMS), family and loved ones, and other important communications.

Putting URLs or phone numbers or both in a WEA message will encourage message recipients to attempt even more voice calls or data sessions on an already taxed network, thereby compounding the congestion problem. It is almost the equivalence of a “denial of service” attack propagated by the WEA message URL or phone number itself. While the goal of enhancing public safety is important, this proposal risks harm to public safety by congesting networks and potentially making essential lifesaving services inaccessible to citizens in need.

²⁵ CMSAAC Report at § 5.3.2.1

The Notice suggests that inclusion of this information in the alert will minimize “milling behavior.”²⁶ Milling behavior is common in an emergency. A WEA message is designed to provide immediate lifesaving information and does not provide “updates” over time – so certainly the expectation is that the public will seek out other sources to find out more information about what is happening, especially over time. CMSPs are concerned that other sources are not always available when the WEA Alert goes out; that is, radio or TV is not providing the needed coverage of the reason for the alert message. The assumption that providing one single URL in the WEA message will change the behavior of the public not to search beyond that single URL to other sources — including broadcast radio and TV, social media, and other web pages — is not a good one.²⁷

The Notice also asks if WEA messages should include multimedia.²⁸ Existing cell broadcast technologies support text broadcast only, not multimedia. Full multimedia content requires new technologies like evolved Multimedia Broadcast Multicast Service (“eMBMS”) to be deployed. eMBMS standards do not currently support WEA, and a standards effort will be required to determine the feasibility of incorporating WEA capabilities into eMBMS. In addition, it is unlikely that any future eMBMS deployments will have the same coverage as WEA today, nor will all devices likely support eMBMS. eMBMS also has capacity and spectrum implications that require further consideration. For instance, eMBMS “borrows” a portion of the available radio

²⁶ Notice at ¶ 26 n. 46. “Milling” is a behavior in which “individuals interact with others to confirm information and develop a view about the risks they face at that moment and their possible responses. Milling creates a delay between the time a warning is received and the time protective action is taken.”

²⁷ If the rules are adopted allowing for use of phone number or URLs, AT&T stresses that inclusion of that metadata must require the information transmitted be accurate, timely, and provide information relevant to the recipient at the location where the alert is received at the time the individual requests it. That is, not a pointer to a generic web page with no relevant information, or to an unanswered phone number.

²⁸ Notice at ¶ 30.

resources and assigns it to the multimedia broadcast, which would result in a reduction of network resources available for voice and data communications as well as the WEA messages themselves.

To display a map associated with a WEA alert, several pieces of data are required in the mobile device: the map itself, which may or may not be preloaded; the location of the mobile device, which is dependent on user setting; and the coordinates of the alert area (“polygon”). Each of these pose technical challenges that affect the ability to provide a map capability. Getting the coordinates to the mobile device requires the network to broadcast those coordinates, which may take up many if not most (or even require more) of the 360 characters available in one WEA message. New cell broadcast message categories have to be developed to identify this metadata as being coordinate information, new mobile devices are required to receive and process that metadata. Then, the device needs to determine if it is in that polygon using its location-based services (potentially using additional network-based resources), if available. A map has to be constructed and the polygon displayed appropriately. All this will result in delays for the recipient receiving the imminent threat information and trying to take appropriate action.

Photos and the like are not supported and cannot be supported using the existing cell broadcast technologies. The cost associated with eMBMS deployment may also be cost prohibitive especially to smaller carriers, putting those who live or travel to rural areas at a disadvantage.

While AT&T acknowledges technologies such as eMBMS are a potential for WEA multimedia messages, eMBMS has not been deployed and, being driven by commercial business needs, is unlikely to be widely deployed for some time. In addition, eMBMS will likely not achieve as widespread a deployment as LTE owing to its cost, technical requirements (including more spectrum), and the service-specific nature of eMBMS.

Transmitting large amounts of data will add delay to the delivery, as well as decrease battery life. The magnitude of the delay and the decrease in battery life would have to be studied once the type of data to be broadcast is defined. This leads to another problem: the amount of data is dependent on what type of multimedia content would be supported by alert originators. At present, this is unknown because generating multimedia alerts is not supported. There is the potential that this proposal would result in a significant increase in the amount of data to be transmitted.

F. Multilingual WEA Messages

The Notice asks if technical problems continue to limit the ability of Participating CMSPs to provide alerts in languages other than English. In short, the same technical complexities of supporting multiple languages that existed in 2008 still exist today, as the fundamental cell broadcast technology is the same.²⁹ Specifically, CMSAAC identified the following challenges to supporting multiple languages:³⁰

- Fundamentally, the existing air interfaces of CMSPs have technical limitations and the support of multiple languages may result in a significant impact to capacity and latency due to these limitations.
- How many languages should be supported? According to the CMSAAC, only Spanish exceeds 1% of households on a national basis. On a local basis, however, there are potentially more than 37 languages that exceed 1% of households, which would require more than 16 different character sets to be supported in the mobile device. This raises issues such as character set limitations, the amount of CMAS alert message traffic that would need to be delivered in multi-languages, bandwidth limitations, increased cost and complexity, mobile device capabilities and deployment impacts. Additional character sets to support 32 multiple languages also will potentially limit the amount of data that can be transmitted; for example, some character sets require two bytes per character versus one byte per character, and thus 90 characters available in the WEA message now reduces the WEA text message to 45 characters.

²⁹ While there have been significant advances in network capabilities, the underlying design principles of the network remain unchanged, especially the cell broadcast mechanism.

³⁰ CMSAAC Report at § 5.7.

To further complicate support for multiple languages, each language must be broadcast in the 90-character message in the desired language. If the Commission adopts the 360 character extension for LTE networks, there is also the requirement to broadcast the message in that desired language with 360 characters. For example, if the Commission required WEA to support Spanish in addition to English, this requires the alert originator to generate four messages (*i.e.* two per language) – one in English, and one in Spanish, and one for each length (90 and 360 characters). Each additional language requires the generation of two additional WEA messages. The CMSP Infrastructure needs to broadcast each message, in each language and each message length, on its infrastructure. This adds delay to the overall message delivery. Adding additional languages increases the number of messages, aggravating the problem. Moreover, carriers do not know which customers read languages other than English, meaning they must send all messages to all customers. Increasing the number of messages customers receive to account for languages they do not read will only encourage all consumers to opt-out of the messages.

AT&T agrees with FEMA in recommending that WEA, if enhanced to support delivery of alert messages in languages other than English, must require that the alert be generated and made available by the originator in other languages. That is, language translation is not and should not be a function of the CMSP infrastructure or mobile devices.

III. WEA Geo-Targeting

The Notice proposes to revise the Commission’s rules to require that Participating CMS Providers must transmit any alert message that is specified by a geocode, circle, or polygon to a target area not larger than the specified geocode, circle, or polygon.³¹ AT&T does not favor this proposal. AT&T supports a CMS Provider geo-targeting a WEA Alert to the best approximation

³¹ Notice at ¶ 37.

of the polygon, circle, or geocode provided by the alert originator. Specifying it to be “not larger” than the alert area may actually provide a significant “undershoot” of the alert polygon as the CMSP may have to choose to exclude cell sites on the polygon border, or even just outside the polygon, to get the best approximation of that polygon. In addition, cell sites within the polygon may transmit beyond the boundaries of the polygon, and the proposed rule would force CMSPs to withdraw those cells from the WEA transmission. As the alert polygon gets smaller than a single cell site, it would be impossible to transmit the WEA Alert and still meet this requirement to be no larger than the alert polygon.

Some parties have argued that finer geo-spatial targeting is necessary to ensure the effectiveness of WEA Alert Messages, which may remain suppressed until they can be distributed to finer geospatial targeted populations so that messages only reach the people who are at risk.³² Yet, those parties have not explained how less finely targeted WEA messages are ineffective. In fact, other alert dissemination methods transmit to geographic areas that are significantly broader than the alert area. For example, television stations, which have broadcast areas that often cover multiple counties, may interrupt regular programming for severe weather coverage in counties far removed from the area at risk. Doubtless, improvements may always be made; but, WEA should not bear the burden (and expense) of geo-targeting complexities to a level unprecedented with other alert dissemination methods.³³

Nor will finer geo-targeting open opportunities for other alert providers.³⁴ Improved geo-targeting does not provide any further opportunities for CMSPs to offer “mass notification” services. The underlying cell broadcast technology – not WEA - provides opportunities for CMSPs

³² *Id.* at ¶ 41.

³³ “The best is the enemy of the good.” Voltaire, *La Béguéule* (*Contes*, 1772)

³⁴ Notice at ¶ 41. In the first place, WEA must remain as a service that is used by federal, state, local and tribal officials to provide imminent threat alerts to the public. Mass notification products, especially those of a commercial

to enter business relationships with mass notification providers, localities, employers, and schools to offer a service using underlying cell broadcast capabilities. In fact, this was the original intent of cell broadcast when originally developed as part of the GSM family of standards and first demonstrated in 1997. The Commission should not look at leveraging WEA for bringing non-WEA alert services to communities, but should encourage industry to explore ways to use cell broadcast as it was designed to do in a commercial setting. Extending cell broadcast services beyond the alerting community is not a function of WEA or “improved geo targeting”.

IV. Alert Logging and Test Reporting

The Notice observes that CSRIC IV concluded there is no established procedure for Participating CMS Providers to inform alert originators or government entities of the success or failure of WEA tests under the current WEA testing model and, thus, no available method to analyze these results in the interest of public safety.³⁵ To remedy this, the Commission proposes to adopt a new Section 10.320(g) that would require Participating CMS Provider Alert Gateways to:

- Provide a mechanism to log messages with time stamps that verify when messages are received, and when the messages are acknowledged or rejected by the Participating CMSP
- Provider Alert Gateway, and if an alert is rejected, to provide the specific error code generated by the rejection;
- Maintain an online log of active and cancelled alert messages for 90 days, and maintain archived logs for at least 36 months that should be accessible by Participating CMS Providers for testing and troubleshooting purposes; and
- Generate monthly system and performance statistics reports based on category of alert, alert originator, alert area, and other alerting attributes.³⁶

nature, should not be considered associated with WEA in any way, as that opens the door for security risks and ultimately affecting the integrity of WEA

³⁵ Notice at ¶ 55.

³⁶ Notice at ¶ 56.

AT&T supports these requirements, which are currently supported in ATIS/TIA standards. As the Commission notes, these logging requirements were recommended by the CMSAAC after extensive efforts to arrive at a consensus among CMS Providers, vendors, public safety entities, organizations representing broadcast stations, and organizations representing people with disabilities and the elderly. The CMSP Gateway is capable of performing these logging functions.

In addition, the FEMA IPAWS Gateway should also have responsibility to perform logging of the essential information described above. IPAWS should log messages with time stamps that verify when messages are received from the alert originator, and when the messages are acknowledged or rejected by the Participating CMSP (with specific error codes as necessary). IPAWS should maintain an online log of active and cancelled alert messages for 90 days, and maintain archived logs for at least 36 months; these archived logs should be accessible by Alert Originators and Participating CMS Providers for testing and troubleshooting purpose. IPAWS should generate monthly system and performance statistics reports based on category of alert, alert originator, alert area, and other alerting attributes.

To develop a full view of how the WEA system is working, from alert initiation to receipt of the message by the mobile device, the Notice proposes that CMSPs create a log of when the alert is received by, for example, a mobile device controlled by and in the possession of the Participating CMS Provider. While AT&T already does selectively monitor receipt of WEA required monthly tests (“RMTs”) by representative, dedicated, end-user devices controlled by and in its possession, it is impossible to support monitoring over a network comprised of tens of thousands of cell sites.

As an alternative, AT&T proposes that a log of successful broadcasts by the Radio Access Network associated with the WEA test message is sufficient to provide the full view of the WEA

system. That is, it can be concluded that if the Radio Access Network is successfully broadcasting the WEA test message, then it can also be concluded that the mobile devices served by the cell sites broadcasting the WEA test message are successfully receiving the message. AT&T is concerned that giving broad access to this log can result in misinterpretation of the data from the Participating CMSP network. Authorized entities should have access to the logs on an as-needed basis. Instead giving broad access to the test logs, AT&T suggests that stakeholder representatives (individual Participating CMSPs, FCC, FEMA, NWS, etc.), should, as necessary, meet to share and discuss logging data. Individual Participating CMSPs should not be required to share data with other CMSPs.

WEA reporting should be required only for RMTs, not localized tests. AT&T regards the burden of a test reporting process as one that should be spread across the entire WEA system: alert originators, FEMA IPAWS, and Participating CMSP Providers. All stakeholders in the WEA system should be responsible for reporting on their respective responsibilities for WEA testing. The WEA stakeholders should define the test reporting procedure, what form should that reporting should take, and what specific information should be reported by each stakeholder. Some aspects, such as geo-targeting, are not available because of the nature of cell broadcast, radiofrequency physics, and cell site geography. Indeed, the accuracy of geo-targeting is not readily available other than by comparing the polygon supplied by the alert originator and manually looking at the cell sites where the test message was broadcast. This is manually intensive on the part of the Participating CMSP. Other aspects, such as alert delivery latency, are an end to end system function requiring data from all stakeholders. Subjective measurements such as the quality of public response may not be available at all through testing, and are subjective at best.³⁷

³⁷ To generate WEA reports as an industry, AT&T proposes that an industry organization aggregate and anonymize WEA test data. Any reporting requirement should be on an annual basis.

The Commission should not specify the mechanisms or technology used for test reporting. The method Participating CMSPs use should be the CMSP's choice; the Commission should specify only the type of information in the test report and the report frequency. AT&T does not support third party APIs to satisfy test reporting requirements because there are significant security and privacy issues with having third party software perform this function.

V. Provisions Affecting Participating CMS Providers and Subscribers

AT&T agrees that the number of consumers opting out of WEA should receive more attention than it does. However, AT&T does not have sufficient information to explain why consumers opt out of WEA.³⁸ To illustrate the lack of information about possible factors leading to consumer opt out, consider that in the early days of WEA, county level geo-targeting was an issue. However, the major Participating CMSPs have since geo-targeted to the best approximation of the supplied polygon, which has significantly reduced the geo-targeting issue. Clearly, more work needs to be done before any conclusions are reached or rule changes made.

The FCC also proposes to amend its rules to allow the broadcast or transmission of the WEA Attention Signal as part of government-developed Public Service Announcements (“PSAs”) to address alert originators’ need to raise public awareness about WEA.³⁹ AT&T supports modification of the Commission’s rules to allow WEA alert tones to be used in PSAs, whether by FEMA, alert originators, or even industry (including Participating CMSPs). The company does not believe they should be subject to review. By contrast, EAS tones should not be treated in the same fashion because EAS receivers can be triggered by the tones if they appear on radio or TV broadcasts.⁴⁰

³⁸ For example, it is not known how many consumers opt out of WEA or their reasons for doing so. These statistics are not available to the Participating CMSP because they are consumer choices made on the mobile device.

³⁹ Notice at ¶ 70.

⁴⁰ WEA tones, while they use the same frequencies, have a cadence that is unique to WEA.

Finally, with the exception of the Presidential Alert, AT&T recommends that WEA Alerts continue to be processed on a first-in-first-out (“FIFO”) basis. This prioritization is performed at the CMSP Gateway and, because of the nature of cell broadcast technology, it is not possible to prioritize WEA messages over other activities taking place on a mobile device. WEA is data broadcast over the control channel of the device, whereas other data traffic is transmitted over data channels. Without a re-design of the entire system, it is not possible to prioritize WEA messages on anything other than a FIFO basis.

CONCLUSION

For the foregoing reasons, AT&T supports increasing the maximum number of characters in a WEA message from 90 to 360 on 4G LTE networks, while maintaining the current 90-character limit for 2G and 3G devices as the Commission proposes. In addition, AT&T supports the creation of a new category, Emergency Government Information, as proposed in the Notice. In supporting the creation of this new category, AT&T emphasizes the need for FEMA to continue to vet and train all alert generators including those who will create Emergency Government Information alerts. Owing to the complexity and potentially baleful effects upon CMPS networks, AT&T, while it supports generating WEA messages in English and Spanish, does not support generating those messages in multiple, other languages.

AT&T also opposes several other suggestions made in the Notice because of the effects these proposals would have upon the CMPS networks, the delivery time of the alerts, and the cost these enhancements would impose upon small and rural carriers. AT&T urges the Commission to recognize that WEA is a “bell ringer” service meant to get the attention of members of the public so that they can seek additional sources of information. WEA should not be over-burdened with an expanded mission for which it was not created.

Respectfully submitted,



By: William L. Roughton, Jr.
Robert Vitanza
Gary L. Phillips
David Lawson
1120 20th Street, N.W.
Suite 1000
Washington, D.C. 20036
(202) 457-2040
Counsel for AT&T Services, Inc.

January 13, 2016

APPENDIX 1

Increasing Maximum WEA Character Length	
Standard & Optional Description	Associated Updates
<p>3GPP TS 23.041 Technical realization of Cell Broadcast Service</p> <p>This is the 3GPP specification for Cell Broadcast service includes the global requirements for the Commercial Mobile Alert Service (CMAS) and is the underlying network enabler for WEA.</p> <p>Updates to Joint ATIS/TIA and ATIS WEA specs dependent on update to 3GPP TS 23.041.</p>	<p>Update to indicate support for both 90 and 360 character messages.</p> <p>May require updates to define additional cell broadcast message identifier values for the 360 character alert messages.</p>
Other 3GPP specifications	TBD
<p>J-STD-100 Joint ATIS/TIA CMAS Mobile Device Behavior Specification</p>	<p>Update to support both 90 and 360 character WEA alert messages</p> <p>Update to define relationship between 90 and 360 characters WEA alert messages (e.g., what if mobile device receives both, what if roaming from 360 character area to 90 character area)</p>
<p>J-STD-101 Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification</p> <p>This spec defines C interface between FEMA and CMSP.</p>	Update to support both 90 and 360 character WEA alert messages.
<p>J-STD-101.a Supplement A to J-STD-101, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification</p> <p>This supplement defines the C1 interface.</p>	Update to align with the changes to J-STD-101.
<p>J-STD-102 Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Test Specification</p> <p>This is the test specification for certification of C-Interface between FEMA and CMSP for 90 character WEA alert messages.</p>	<p>Update to add test cases for sending only 360 character WEA alert messages across the C Interface.</p> <p>Update to add test cases for sending both 90 and 360 character WEA alert messages across the C Interface in the same message.</p>
<p>ATIS-0700008 Cell Broadcast Entity (CBE) to Cell Broadcast Center (CBC) Interface Specification</p> <p>This spec defines an interface and message format for Cell Broadcast messages from the CBE to the CBC. The 3GPP specs do not define this interface. The CBE is the entity which creates the Cell Broadcast messages for broadcast by the CBC. In WEA, the CMSP Alert Gateway is the CBE.</p>	Update to support both 90 and 360 character WEA alert messages.
<p>ATIS-0700010 CMAS via EPS Public Warning System Specification</p> <p>This spec defines the support of WEA via LTE.</p>	Update to support both 90 and 360 character WEA alert messages.

Increasing Maximum WEA Character Length	
Standard & Optional Description	Associated Updates
ATIS-0700021 Canadian Wireless Public Alerting Service (WPAS) LTE Mobile Device Behavior	Updates may be required to align with the updated J-STD-100 spec.
ATIS-07000xx CMAS International Roaming Specification This spec defines WEA support for inbound and outbound roamers. Currently in Letter Ballot Review.	Update to support both 90 and 360 character WEA alert messages.

APPENDIX 2

Classifying Emergency Government Information (if Opt-Out or Additional Alert Classes Required)	
Standard & Optional Description	Associated Updates
<p>3GPP TS 23.041 Technical realization of Cell Broadcast Service</p> <p>This is the 3GPP spec for Cell Broadcast service includes the global requirements for the Commercial Mobile Alert Service (CMAS) and is the underlying network enabler for WEA.</p> <p>Updates to Joint ATIS/TIA and ATIS WEA specs dependent on update to 3GPP TS 23.041.</p>	<p>Update to assign new cell broadcast message identifiers for Emergency Government Information WEA messages</p> <p>Update for new additional C-Interface message event codes for the new alert classes for Emergency Government Information WEA messages.</p>
Other 3GPP specifications	TBD
<p>J-STD-100 Joint ATIS/TIA CMAS Mobile Device Behavior Specification</p>	<p>Update to support receiving Emergency Government Information WEA messages.</p> <p>Update to support subscriber opt-in/opt-out of Emergency Government Information WEA messages based upon new cell broadcast message identifiers as defined in the updated 3GPP TS 23.041.</p>
<p>J-STD-101 Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification</p> <p>This spec defines C interface between FEMA and CMSP.</p>	Update to support new C-interface message event codes for the new alert classes for Emergency Government Information WEA messages.
<p>J-STD-101.a Supplement A to J-STD-101, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification</p> <p>This supplement defines the C1 interface.</p>	Update to align with the changes to J-STD-101.
<p>J-STD-102 Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Test Specification</p> <p>This is the test specification for certification of C-Interface between FEMA and CMSP.</p>	Update to add test cases for the C-interface messages with new C-Interface message event codes for Emergency Government Information WEA messages.
<p>ATIS-0700008 Cell Broadcast Entity (CBE) to Cell Broadcast Center (CBC) Interface Specification</p> <p>This spec defines an interface and message format for Cell Broadcast messages from the CBE to the CBC. The 3GPP specs do not define this interface. The CBE is the entity which creates the Cell Broadcast messages for broadcast by the CBC. In WEA, the CMSP Alert Gateway is the CBE.</p>	Update to support new C-interface message event codes for Emergency Government Information WEA messages.
<p>ATIS-0700010 CMAS via EPS Public Warning System Specification</p> <p>This spec defines the support of WEA via LTE.</p>	Update to support new cell broadcast message identifiers for Emergency Government Information WEA messages based upon new cell broadcast message identifiers defined in the updated 3GPP TS 23.041.
<p>ATIS-0700021 Canadian Wireless Public Alerting Service (WPAS) LTE Mobile Device Behavior</p>	Updates may be required to align with updated J-STD-100 spec.

Classifying Emergency Government Information (if Opt-Out or Additional Alert Classes Required)	
Standard & Optional Description	Associated Updates
<p>ATIS-07000xx CMAS International Roaming Specification</p> <p>This spec defines WEA support for inbound and outbound roamers.</p> <p>Currently in Letter Ballot Review.</p>	<p>Update to support new cell broadcast message identifiers for Emergency Government Information WEA messages based upon new cell broadcast message identifiers defined in the updated 3GPP TS 23.041</p> <p>Update to support the new event codes for the new alert classes for Emergency Government Information WEA messages.</p>