October, 2014 WORKING GROUP 2

Geographic Targeting, Message Content and Character Limitation Subgroup Report

Table of Contents

List of Figures

List of Tables

1 Results in Brief

1.1 Executive Summary

The group was challenged by the prospect of enhancing Wireless Emergency Alerts (WEA) without harming commercial wireless networks, which voluntarily elected to transmit WEA Alert Messages to their subscribers. Members of the alert origination community desire improvements which would personalize the threat and improve public response to WEA Alert Messages based on outcomes from social science studies and long known tenets of public alerting. The most desired improvements include increased message length, supplementing the WEA with graphical information (e.g., display of the recipient's locations along with a map of the threat area, photo of a suspect, missing child, etc.), and improving the geographical targeting granularity.

Wireless industry members recommend that the FCC focus on enhancements to the existing WEA rules which are technology neutral. The wireless industry also recommends that enhancements be consistent with 4G LTE technology which is the predominant cellular technology. Wireless industry members were most concerned about feasibility and impacts to cellular networks and improvements which would be consistent with their voluntary election to participate in WEA and do not violate their obligations to the WARN Act, especially in the area of liability protection.

There was consensus among the group to recommend the FCC modify their rules to increase the maximum WEA Alert Message length consistent with capabilities of 4G LTE (approximately 280 displayable characters subject to technology confirmation by ATIS/TIA standards).

Obtaining consensus on supplementing the WEA with graphical information and enhancements to geographical targeting is more challenging. Members of the alert origination community suggest that the built-in capabilities of mobile devices (e.g., location finding, maps, Internet connectivity, etc.) be leveraged in order to achieve the desired improvements. The wireless industry expresses great concern about the feasibility of providing graphical information since standards-based WEA uses cell broadcast which only supports text messages, and other solutions may have potential negative impacts to CMSP infrastructure. Ultimately, an ATIS/TIA feasibility study is recommended to consider several alternatives as well as potential impacts to CMSP networks. Concerns are also raised about Intellectual Property Rights issues which may preclude advancements to WEA, most notably with regard to geographical filtering of alerts at the device level. CSRIC WG2 recommends that the FCC should work to address these issues.

Recommendations are also made which focus on the use of best practices by CMSPs for cell broadcast geographical targeting and by Alert Originators for alert message content.

2 Introduction

2.1 Overview

This report is from the sub-working group that is analyzing geo-targeting, message content

and character limitations of Wireless Emergency Alerts (WEA)[1].

The structure of this report is as follows:

- Executive Summary.
- Section 2 contains the overview, the organization chart, the working group members, and the working group objective.
- Section 3 provides background information on the following topics:
    - Regulation & Statutes
    - Currently Deployed WEA
    - Issues and Challenges with Current WEA
    - Status of Wireless Network Deployment
- Section 4 contains the subgroup analysis, findings, and recommendations and is organized as follows:
    - Assumptions and Objectives for Enhancing WEA
    - Summary of DHS Studies on Mobile Alerting
    - Analysis and Findings on Message Length
    - Analysis and Findings on Message Content
    - Analysis and Findings on Geo-Targeting
    - Topics for Further Study
    - Subgroup Recommendations
    - Impact to Standards
- Section 5 contains the conclusions.
- Appendix A enumerates the existing standards for WEA.
- Appendix B contains the findings and recommendations from the DHS studies on mobile alerting.
- Appendix C identifies potential alternatives for WEA Alert Message length options.
- Appendix D is an evaluation of WEA geo-targeting options.
- Appendix E provides some examples of alert broadcasting scenarios with emphasis on the geo-targeting aspects.
- Appendix F contains an evaluation of a future mobile alerting concept.
- Appendix G provides a list of acronyms used in this report.

[1]On February 25, 2013, the FCC issued an order revising Part 10 of its rules by changing the name "Commercial Mobile Alert System" (CMAS) to "Wireless Emergency Alerts" (WEA) in order to more accurately reflect common parlance and thus reduce confusion. (*See* The Commercial Mobile Alert System, PS Docket No. 07-287, *Order*, 28 FCC Rcd 1460 (rel. Feb. 25, 2013). Both "CMAS" and "WEA" are used throughout this document and refer to wireless emergency alerts.

- Appendix H provides definitions for terminology used in this report.

2.1.1 Organization Chart

Communications Security, Reliability, and Interoperability Council (CSRIC) IV									
CSRIC Steering Committee									
Chair or Co-Chairs: Working Group 1	Chair or Co-Chairs: Working Group 2	Chair or Co-Chairs: Working Group 3	Chair or Co-Chairs: Working Group 4	Chair or Co-Chairs: Working Group 5	Chair or Co-Chairs: Working Group 6	Chair or Co-Chairs: Working Group 7	Chair or Co-Chairs: Working Group 8	Chair or Co-Chairs: Working Group 9	Chair or Co-Chairs: Working Group 10
Working Group 1: Next Generation 911	Working Group 2: Wireless Emergency Alerts	Working Group 3: EAS	Working Group 4: Cybersecurity Best Practices Working	Working Group 5: Server-Based DDoS Attacks	Working Group 6: Long-Term Core Internet Protocol Improvements	Working Group 7: Legacy Best Practice Updates	Working Group 8: Submarine Cable Landing Sites	Working Group 9: Infrastructure Sharing During Emergencies	Working Group 10: CPE Powering

2.1.2 Working Group 2 Membership

Table 1: CSRIC Working Group Team Members

Name	Organization
Brian K. Daly, Co-Chair	AT&T
Mike Gerber, Co-Chair	NOAA/National Weather Service
William B Anderson (advisory)	Carnegie Mellon Software Engineering Institute
Keith Bhatia	Telecommunication Systems
Cedric Cox	Intrado
John Davis	Sprint
Tim Dunn	T-Mobile US
Brad Gaunt	Sprint
Dan Gonzalez	RAND
Denis Gusty	Department of Homeland Security, Science and Technology Directorate
Craig Hodan	NOAA
Robert Hoever	National Center for Missing & Exploited Children
Brian Josef	CTIA
Mark Lucero	Department of Homeland Security - FEMA
Hisham Kassab	Mobilaps, LLC
Farrokh Khatibi	ATIS (Qualcomm)
John Kopec	Sprint
John Madden	State of Alaska
Matt May	Wyandotte County Kansas Emergency Management
Hutch McClendon	Advanced Computer and Communications, LLC
Peter Musgrove	ATIS (AT&T)

Name	Organization
Mehran Nazari	Rural Wireless Association
Orlett W. Pearson	Alcatel-Lucent
Ganesh Ramesh	Telecommunication Systems
Nag Rao	ATIS (Nokia Networks)
Larry Rybar	Verizon Wireless
Francisco Sanchez, Jr.	Harris County Office of Homeland Security & Emergency Management
Matthew Straeb	Global Security Systems/ALERT FM
Kim Titus	NQ Mobile
Xiaomei Wang	Verizon Wireless
James Wiley	FCC

Also, DeWayne Sennett of AT&T served as Document Editor and Document Manager for the development of this CSRIC subgroup report.

2.2 Objective of CSRIC IV Working Group 2 Subgroup

The Communications Security, Reliability and Interoperability Council (CSRIC) Working Group 2 (WG-2) Geographic Targeting, Message Content and Character Limitation Subgroup is tasked with making recommendations on geographic targeting, message content and message length of WEA Alert Messages. This subgroup is part of the larger WG-2 which has also been tasked to make recommendations on WEA testing, other potential types of WEA alerts (e.g., audio streaming, video streaming and multimedia), and alerting to people with disabilities. These tasks are identified in the "CSRIC IV Descriptions and Leadership" document of August 27, 2013. The document also elaborates on the required considerations, stating that WG-2

> "will review the Commission's current Wireless Emergency Alerts (WEA) rules, taking into account:
>
> (1) experiences with WEA since its deployment on April 7, 2012 (including those of WEA industry participants, the Federal Gateway and Alert Originators),
>
> (2) technological advances since the original WEA technical recommendations were submitted by the Commercial Mobile Service Alert Advisory Committee in 2007, and
>
> (3) other factors, as appropriate, and develop recommendations for CSRIC's consideration for any necessary changes to ensure that WEA continues to serve as a valuable method to alert the public during an emergency."

While the paging community was a member of the FCC CMSAAC for the development of the initial alerting recommendations and paging carriers fall under the definition of Commercial Mobile Service Provider, no paging industry representatives are members of the FCC CSRIC IV committee. Consequently, the needs and positions of the paging community are not reflected in this subgroup report.

3 Background

This section provides background information about the current Wireless Emergency Alerts (WEA) service. For purposes of this document, the term Wireless Emergency Alerts or WEA refers to the current version of the Wireless Emergency Alerts Service. The background information in this section is organized as follows:

- Section 3.1 identifies the applicable regulations and statutes.
- Section 3.2 provides an overview of the currently deployed WEA.
- Section 3.3 describes the issues and challenges with the current WEA including the issues and challenges associated with the current geo-targeting, current message length, and current message content.
- Section 3.4 contains the status of the wireless network deployments.

3.1 Regulations & Statutes

The following table is a listing of the FCC Regulations and the US Statutes related to the implementation of Wireless Emergency Alerts (WEA) in the United States.

Table 2: FCC Regulations and US Statutes

Number	Title	Description
FCC-07-214A1	FCC Notice of Proposed Rulemaking for Commercial Mobile Alert System	This is the FCC NPRM for CMAS. The results of the FCC Commercial Mobile Service Alert Advisory Committee (CMSAAC) are included in this NPRM.
FCC 08-099A1	FCC 1st Report and Order for Commercial Mobile Alert System	This is the FCC 1st Report and Order for Commercial Mobile Alert System. This FCC Report and Order contains the CMSAAC recommendations and defines the general CMAS functional requirements.
FCC 08-164A1	FCC 2nd Report and Order for Commercial Mobile Alert System	This is the FCC 2nd Report and Order for Commercial Mobile Alert System. This FCC Report and Order covers the Digital Television Transmission Towers Retransmission Capability and CMAS Testing Requirements.
FCC 08-184A1	FCC 3rd Report and Order for Commercial Mobile Alert System	This is the FCC 3rd Report and Order for Commercial Mobile Alert System. This FCC Report and Order covers the CMAS election procedures for CMSPs, CMAS withdrawal procedures for CMSPs, and subscriber notification requirements for CMAS.
WARN Act	Warning, Alert, and Response Network (WARN) Act	This is the statute that defined CMAS. The WARN Act is Title VI of H.R. 4954 "Security and Accountability For Every Port (SAFE) Act of 2006".

3.2 Currently Deployed WEA

This section describes the currently deployed WEA. The descriptions below are for standards based deployed WEA. There have been reports of systems and "apps" that emulate

WEA but do not comply with the standards, perhaps used by small CMSPs that find it cost prohibitive to deploy cell broadcast. Such non-standardized systems are outside the control of CMSPs and are not covered in this document.

The WEA currently deployed by FEMA and most Commercial Mobile Services Providers (CMSPs) in the United States is based on standards created in ATIS, TIA, and 3GPP (including joint ATIS/TIA standards). These standards build upon existing standards-defined infrastructure capabilities (e.g., cell broadcast) and were designed to allow Participating CMSPs to comply with the FCC regulations for WEA (see FCC Report and Order references in Section 3.1). New standards were developed to support the interface from FEMA to the CMSPs (the "C" interface in Figure 1 below). Appendix A contains a listing of the major CMAS-related standards (as well as some related FCC documents and the WARN Act) used to support implementation of Wireless Emergency Alerts (WEA) in the United States.

The current Cell Broadcast based WEA solution only broadcasts text messages and is not capable of broadcasting multimedia content.

A functional reference model for WEA is shown in the following figure:

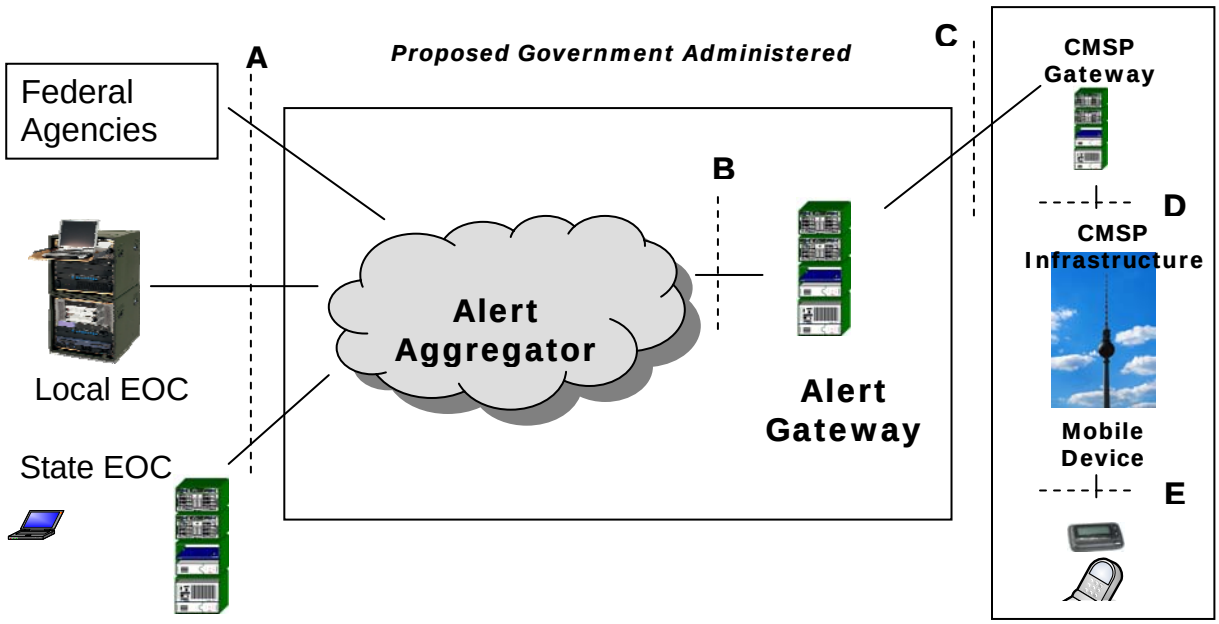


Figure 1: WEA Functional Reference Model

With regard to geo-targeting, while the FCC rules specify county-level targeting, the current standards go well beyond this and allow for a geocode (e.g., a unique identifier for a region), circle or polygon representing the intended target broadcast alert area from the Alert Originator through the FEMA alert aggregator and Federal Alert Gateway to the CMSP gateway. The CMSPs map the intended alert area to the appropriate cell sites and sectors in their network for broadcast transmission of the WEA Alert Message using the standardized cell broadcast capability.

The FCC regulations for WEA require geo-targeting to be performed by the CMSPs on a

county basis, but those regulations also allow CMSPs to geo-target to an area smaller than a county if the CMSP has the capability to geo-target to a sub-county basis. Many CMSPs provided comments to the FCC stating that they would voluntarily geo-target WEA Alert Messages to a sub-county basis, best approximating the alert area polygon given cell broadcast constraints, even with their initial deployments of WEA. Whether a CMSP geo-targets on a county or sub-county basis, the algorithms for mapping the intended alert area to the relevant cell sites/sectors in the CMSP network are considered proprietary and there is no standard method to perform this mapping. Each CMSP handles the mapping in their own proprietary manner, since the geo-targeting capabilities is dependent upon each individual CMSP cell site topology. Section 3.2.1 below provides additional details on current geo-targeting capabilities.

With regard to WEA Alert Message length, the currently deployed WEA offerings by Alert Originators, FEMA, and CMSPs in the United States abide by the 90-character maximum message length required by the FCC regulations and supported in the industry standards. Section 3.2.2 below provides additional details on the current 90-character maximum length for a WEA Alert Message.

Section 3.2.3 below provides details on the derivation of WEA Alert Message content. Message content is the responsibility of the Alert Originator. The currently deployed WEA offerings by CMSPs in the United States support transmission of the WEA Alert Message content as provided on the interface to the CMSP from the FEMA Federal Alert Gateway. The CMSPs do not alter the content of the WEA Alert Message provided by the Federal Alert Gateway, and transmit the WEA Alert Message content as received with no modifications by the CMSP network.

3.2.1 Current Geo-Targeting Capabilities

The term “geo-targeting” refers to the method used for an Alert Originator to identify the alert area and for a CMSP to broadcast the WEA Alert Message to a geographical area that best approximates the alert area. The method used to identify an alert area within the Alert Originator system differs from the method used to identify the broadcast area within the CMSP infrastructure. For example, within the Alert Originator system, the alert area may be identified in the form of a list of counties, polygons or circles. In the CMSP infrastructure, the alert area may be identified in the form of addressable radio transmission sites (e.g., cell sites and/or sectors). Basically, the CMSP infrastructure determines the cell sites/sectors that will broadcast the alert message to a best approximation of an alert area specified by the Alert Originators. More specifically, the term “alert area” refers to the counties, polygons, and circles and the term “broadcast area” refers to the list of cell sites and sectors within the CMSP infrastructure. Additional examples of alert broadcast with emphasis on geo-targeting aspects are provided in Appendix E.

3.2.1.1 Alert Area

Referring to Figure 1, the Alert Originator sends the alert area information to the Federal Alert Gateway over the A & B interface along with other alert information using the Common Alerting Protocol (CAP). The Federal Alert Gateway sends the alert area information to the CMSP Gateway (CMSP-GW) over the C-interface (see Figure 1) per ATIS/TIA standard J-STD-101. Within the CMSP infrastructure, the CMSP-GW sends the

alert area information to the Cell Broadcast Center (CBC) as per the standard ATIS-0700008[2].

J-STD-101 defines that the Federal Alert Gateway passes the alert area information to the CMSP Gateway as a combination of one or more of the following geographic references:

- CMAS_geocode
- CAP_geocode
- Geographic Names Information Systems (GNIS)
- Polygon
- Circle

J-STD-101 defines that the Federal Alert Gateway shall include at least one instance of CMAS_geocode. In the present version of the standards, the inclusion of other methods of defining the alert area is optional and as such the CMSP may or may not support the alert area information in forms other than the CMAS_geocode. However, polygon and circle geo-targeting options are supported by the major US wireless operators.

[2] ATIS-0700008 defines the functionalities for 3GPP based systems such as GSM, UMTS and LTE and not the 3GPP2 based systems such as CDMA and CMDA2000.

3.2.1.1.1 CMAS_geocode

An alert area in the form of CMAS_geocode is basically an extension of FIPS (Federal Information Processing Standard) code and is identified with a 5 character-set, uniquely assigned to a county, region or other equivalent entity. J-STD-101 states that the first two characters of geocode identify the state or region and the last three characters identify the counties, regions or equivalent entities. When the alert area includes the entire country (USA), the geocode value of "00000" is used. When the alert area includes an entire state, the first two characters are used to identify the state followed by three zeroes.

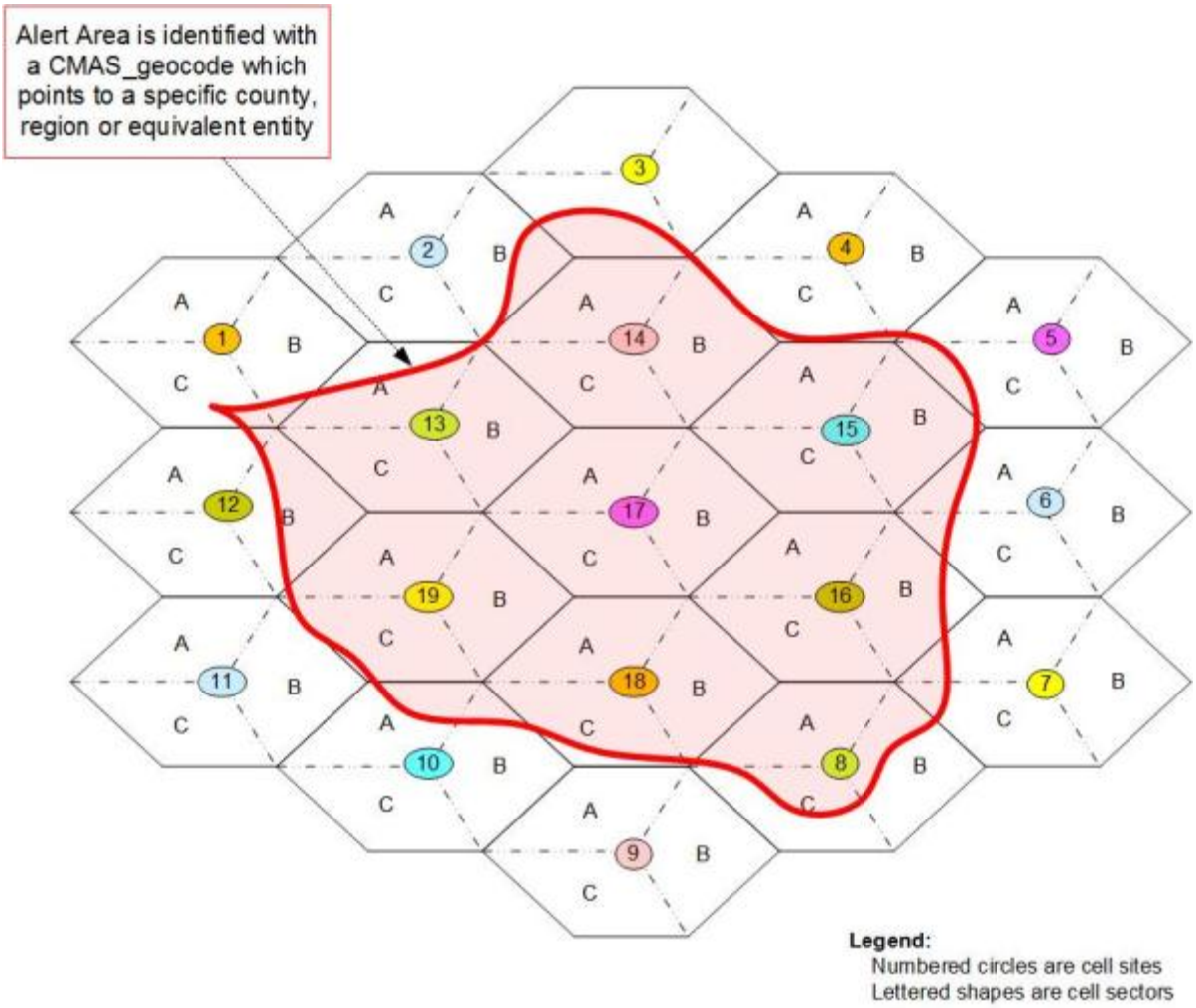


Figure 2: CMAS_Geocode can point to a County, Region or Equivalent Entity

3.2.1.1.2 CAP_geocode

An alert area in the form of CAP_geocode is passed by the Federal Alert Gateway to the CMSP Gateway if the Federal Alert Gateway receives such information from the Alert Originator in the CAP. CAP_geocode consists of six characters and is represented by "PSSCCC" where CCC is the code used to identify the counties, regions or specific entities, and SS is the code used to identify the state or region and P is used to subdivide a county into smaller regions. The contents of the CAP_geocode are defined in the CAP.

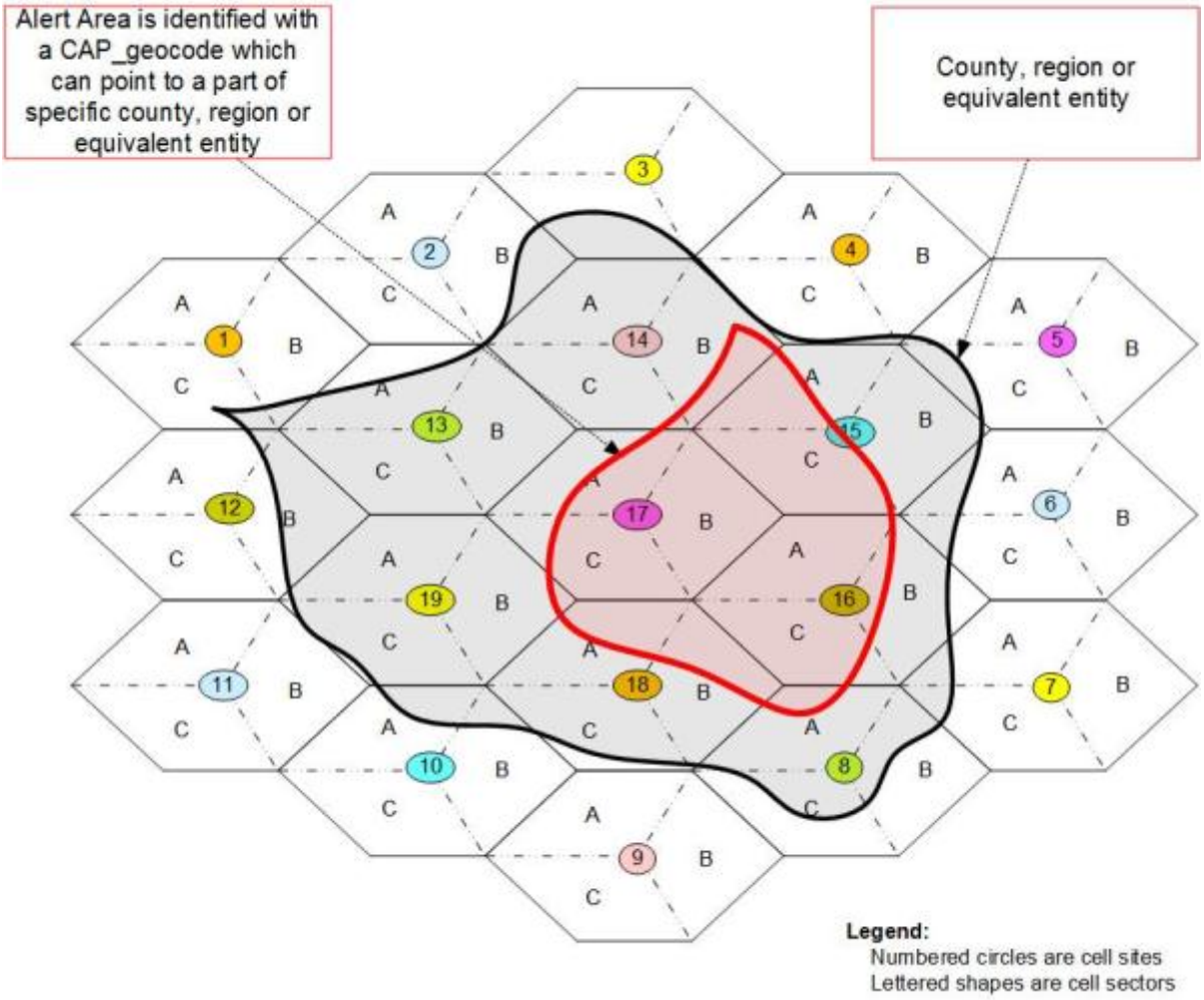


Figure 3: CAP_Geocode can point to a part of County, Region or Equivalent Entity

3.2.1.1.3 GNIS

An alert area in the form of GNIS is identified with a geographic code as per the United States Geological Survey (USGS) Geographic Names Information Systems (GNIS). Basically, this method should be used when a specific point of interest that has a unique code to be used as an alert area.

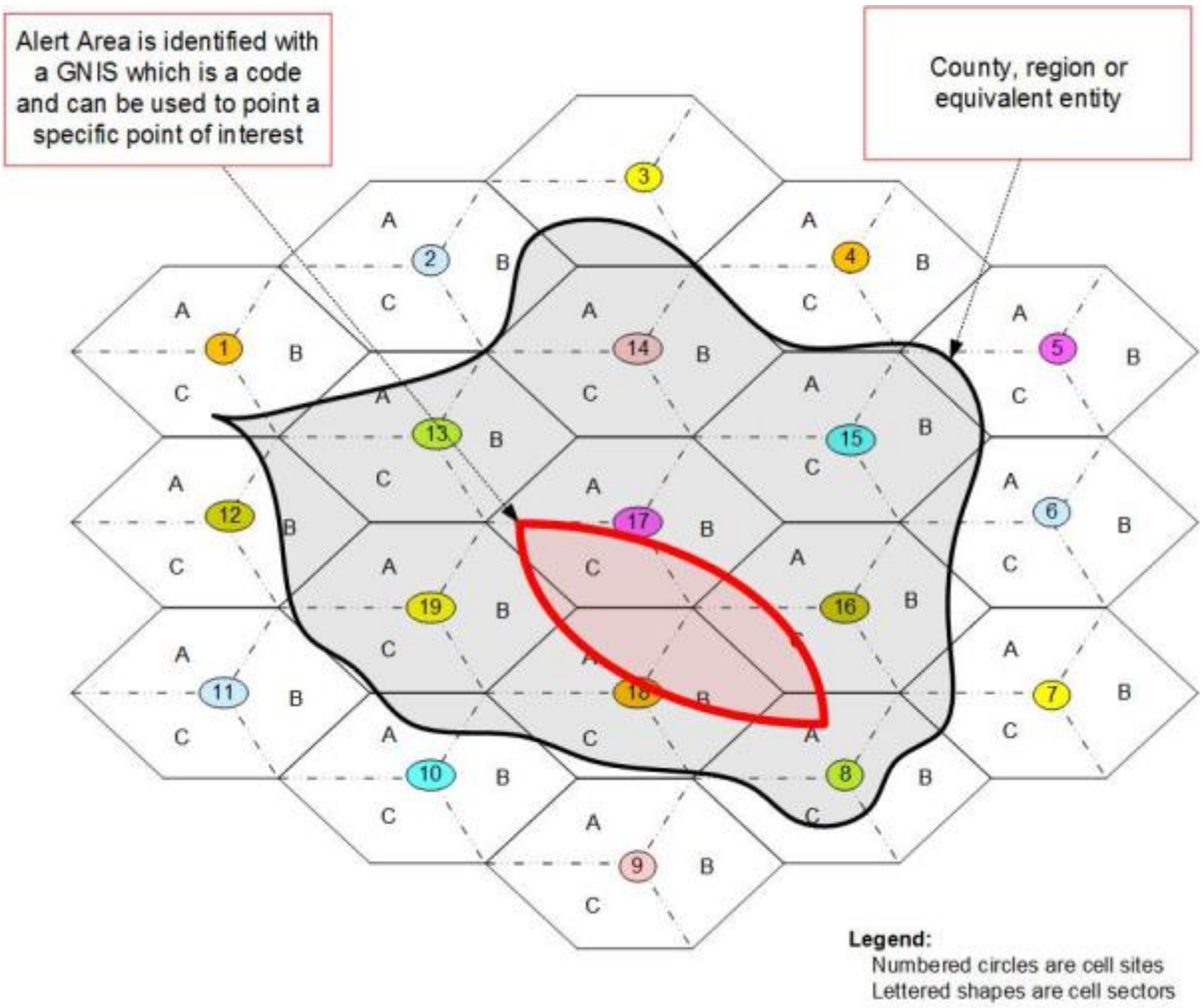


Figure 4: GNIS is a geocode that can point to a Specific Point of Interest

3.2.1.1.4 Polygon

An alert area in the form of Polygon is identified with a series of vertices. Each vertex is identified by a pair of latitude and longitude coordinates. The first and last pairs of coordinates are the same values. Additionally, J-STD-101 states that up to 100 points may be used to specify a polygon as the alert area.

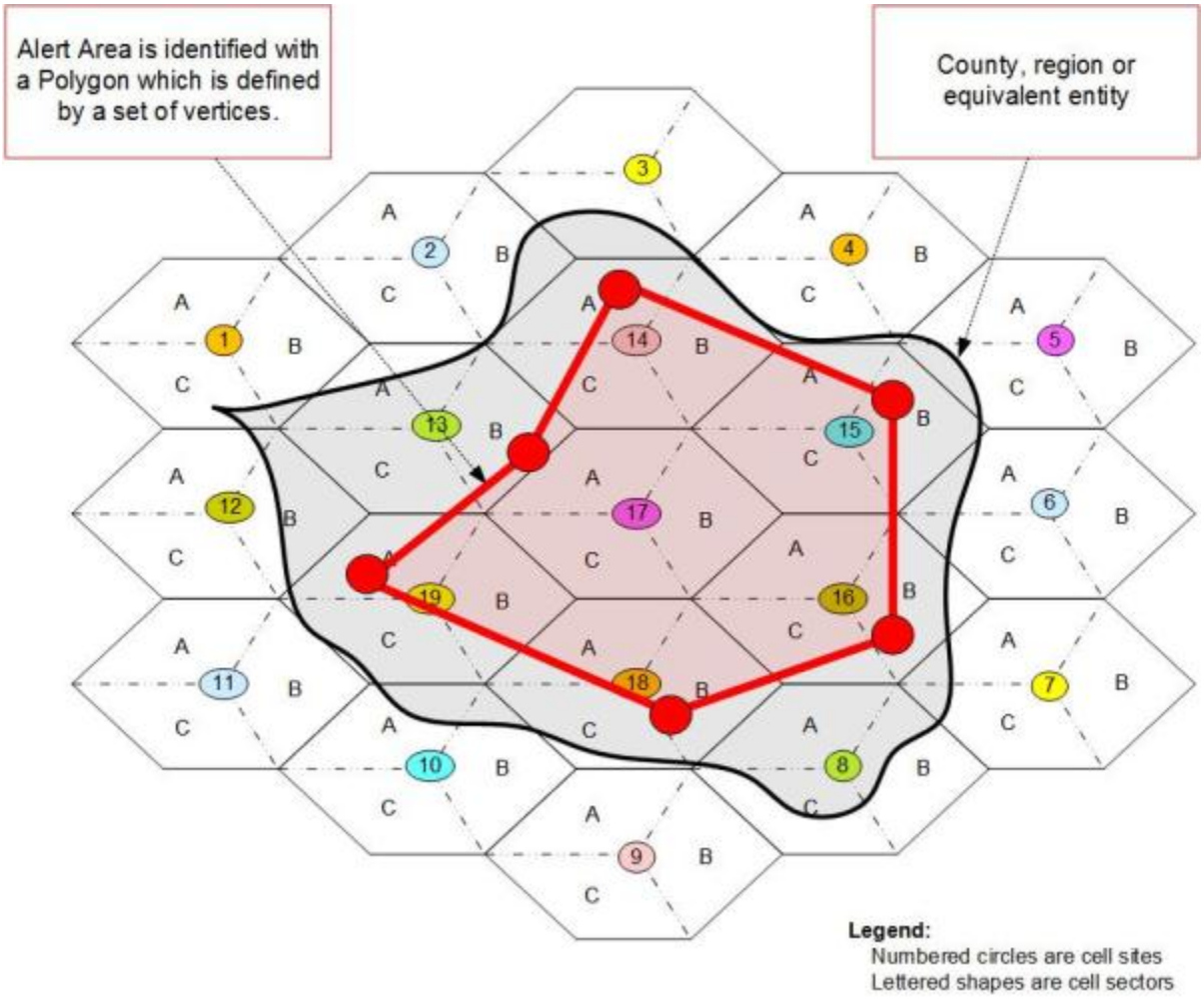


Figure 5: Polygon is defined with a set of points, each with a pair of coordinates

The mapping of Polygon to broadcast area is calculated for each polygon based alert area provided.

3.2.1.1.5 Circle

An alert area in the form of Circle is represented by a central point given as a coordinate pair and a radius value.

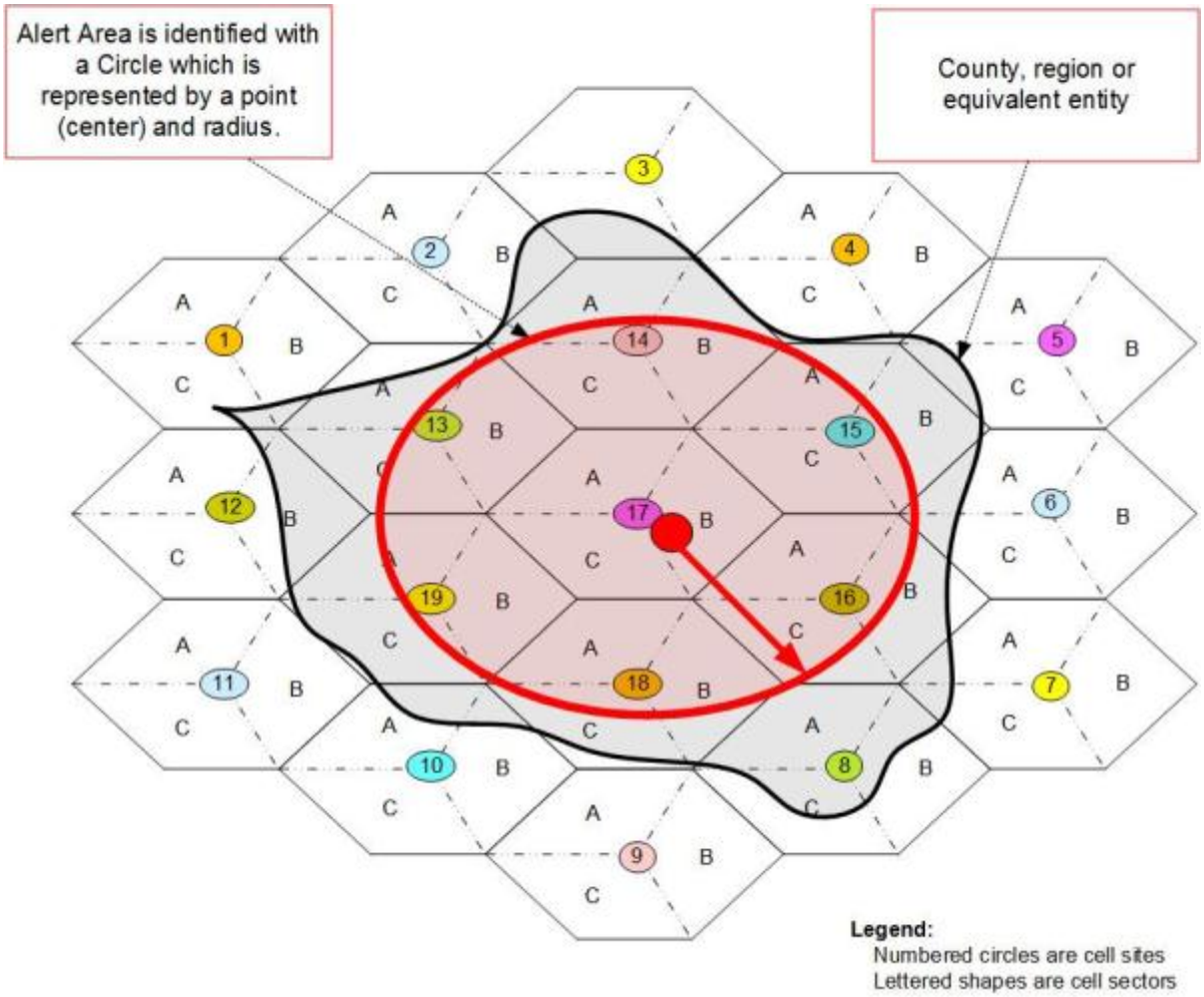


Figure 6: Circle is defined with a point (center) and radius

The mapping of Circle to broadcast area is calculated for each circle based alert area provided.

3.2.1.2 Broadcast Area

Within the CMSP infrastructure, a WEA is broadcast using Cell Broadcast Service (CBS). The Cell Broadcast is a technique used for simultaneous delivery of a message (not necessarily a WEA Alert Message) to multiple users in a specific area.

For CBS based message transmission, the minimum area to which a CBS message can be broadcast is a Cell; and the maximum area to which a CBS message can be broadcast is a list of many Cells. For CBS, a Cell identifies a Sector.

The CBC determines Cells that belong to the broadcast area. The CBC sends the list of Cells

to the broadcasting nodes.

A Cell that belongs to a broadcast area can be determined in at least three ways:

- Based on the location of the physical tower.
- Based on the geographic center (centroid) of the Sector.
- Based upon the radio propagation characteristics of the Cell.

A tower is considered to be within the alert area, if the geographical coordinates of the tower lie within the alert area. A Sector is considered to be within the alert area, if the centroid of the Sector is within the alert area. A Cell is considered to be within the alert area if the estimated radio propagation coverage area overlaps the alert area. There may be other methods implemented to determine the Cells that belong to an alert area.

3.2.2 Current WEA Alert Message Length

In the existing FCC Part 10 WEA rules, the WEA Alert Message length is limited to 90 characters, regardless of the commercial mobile wireless technology or the commercial mobile service provider that provides the WEA. This was done based on recommendations of the CMSAAC to ensure consumers have a common user experience regardless of the device or network. WEA is not to be a "competitive" service across CMSPs, but rather a public service. To that end, the message length was adopted based on the technology with the most restrictive limitation; CDMA2000 in this case. The technology constraints behind this message length limitation exist in deployed networks and have not changed since the CMSAAC analysis. This section will provide a brief technical analysis behind this limitation, confirming the CMSAAC findings. The issues and challenges with the current message length capabilities are discussed in Section 3.3.2.

There are many factors which control the length of a CDMA2000 Broadcast SMS message. The first of these is the speed of the paging channel. If the paging channel is 4800 bps, which is commonly used/deployed for other technical reasons, then the available size of the user part will be 111 octets. However, if the paging channel is 9600 bps rate, then the user part size is 203 octets.

Furthermore, the user part may also include a number of parameters for other purposes. In addition to the actual text message, TIA-637-D standards allows for:

- Service category (like the Message ID in GSM)
- Priority of the message (Normal, Urgent, Emergency)
- Language for the text
- Call Back Number (likely not used in WEA)
- Alert on Message Delivery
- Message Display Mode
- Broadcast Zone ID (where to transmit the message)

If the paging channel is the 9600 bps type, then in the simplest case, wherein the message is a normal priority, in English, with a message center time stamp, 35 octets are needed for parameters and 168 octets are available for the actual message. For 7-bit encoded characters this would result in 192 characters. On the other hand if additional parameters are used (unlikely for WEA), only 139 octets are available for the message. For 7-bit encoded characters this would result in 159 characters.

If the paging channel is the often used and commonly deployed 4800 bps type, then using 35 octets for parameters leaves 76 octets for the actual message. For 7-bit encoded characters this would result in 86 characters for the message itself. With further removal of some unnecessary parameters, the 90 character limit in CDMA2000 for WEA was chosen and led to the CMSAAC recommendation which ultimately was adopted in the FCC Part 10 rules for WEA.

As mentioned earlier, this limitation does not exist in other commercial mobile wireless technologies, such as GSM, UMTS and LTE. Furthermore, LTE is capable of broadcasting more than 90 characters which will be discussed later in this report.

3.2.3 Current Methodologies for Derivation of Message Content

This section describes the current FCC Part 10 rules for the derivation of the message content of WEA Alert Messages. The issues and challenges of the current message content are discussed in Section 3.3.3.

The FCC Commercial Mobile Service Alert Advisory Committee (CMSAAC) was given the assignment to develop recommendations for the alert message content. The needs for individuals with disabilities were considered and evaluated by the CMSAAC in consultation with various advocates for the individuals with disabilities.

The CMSAAC, based on input from consumer stakeholder groups including those representing individuals with disabilities, recommended that the alert messages contain the following information in the order listed:

1. What is happening
2. What area is affected – typically the phrase “in this area” since the affected area is the broadcast area
3. When the alert expires
4. What action should be taken
5. Who is sending the alert

The CMSAAC also recommended that the following guidelines for the generation of the alert message content:

- **Alert Message Content Generated from CAP Message Parameters** -- The CMSAAC report proposed guidelines for the automated generation of the alert

message content based upon the values of the associated CAP message. Annex A of the *Joint ATIS/TIA Federal Alert Gateway to CMSP Gateway Interface Specification* (J-STD-101) contains guidelines for the generation of the alert message in English from the CAP parameters, identifies the CAP parameters to be used for the message generation, and associates CAP parameter values with the recommended phrase for the alert message. Annex A of the *ATIS Implementation Guidelines for CMAS Supplemental Information Retrieval* (ATIS-0700012) contains similar guidelines for the generation of Spanish alert messages from the CAP message.

- **Free Form Message Content** – The CMSAAC report also proposed the generation of free-form alert messages. The CMSAAC recommended that free-form be used for Presidential and Child Abduction alerts and that free-form for Imminent Threat alert messages be used only after the Alert Originators had been sufficiently trained on the generation of free-form alert messages. The CMSAAC also recommended that the free-form alert messages should contain the five components described above and in the recommended order.

For both the generated and the free-form formats of the alert message, there are restrictions on the alert message content. These restrictions were recommended by the CMSAAC after studying the effects on CMSP infrastructure and are defined in the FCC First Report and Order (FCC-08-99A1) and the 47 C.F.R. Part 10 as follows:

> **"§ 10.440 Embedded Reference Prohibition.**
> A CMAS Alert Message processed by a Participating CMS Provider must not include an embedded Uniform Resource Locator (URL), which is a reference (an address) to a resource on the Internet, or an embedded telephone number. This prohibition does not apply to Presidential Alerts."

3.3 Issues and Challenges with Current WEA

This section describes the issues and challenges of the current WEA which are associated with geo-targeting, message character lengths, and message content.

3.3.1 Issues and Challenges with Current Geo-targeting

From the Alert Originator's perspective, ideally all WEA-enabled mobile devices in the geographic area affected by an emergency event would receive the WEA Alert Message broadcast, and no mobile devices outside the defined alert area would receive those particular WEA Alert Message broadcasts. From the Alert Originator's perspective, the more mobile devices outside the affected alert area that receive the WEA Alert Message broadcast, the less precise the geo-targeting.

However, this ideal case cannot be realized using currently deployed Cell Broadcast alone since a cellular network is designed and optimized to handle commercial mobile telecommunications services, and is not designed nor intended to be an optimal geo-targeted emergency alert dissemination network. As a voluntary service offered to Alert Originators and the public, the tools available within the cellular networks will come with limitations.

3.3.1.1 Realities of Geo-Targeting

The cellular network using currently deployed Cell Broadcast alone can only perform an approximation of the alert area. The quality of the cellular network approximation is dependent on many factors including but not limited to the following:

1. Location of the cell tower in relationship to the alert area.

2. Size of the cell radius which is determined by:
    a. RF propagation characteristics
    b. RF power output from the antenna which may vary
    c. Antenna placement and orientation

The placement of cell towers is also based upon many factors including but not limited to the following:

1. RF propagation studies by the cellular operator's network operations departments.

2. Subscriber density (e.g., urban, suburban, or rural).

3. Frequency bands of the licensed spectrum to be used by the cell tower (e.g., 700 MHz bands vs. 1800 MHz bands).

4. Mobile phone traffic patterns which vary based upon time of day and date of week. For example, during the evening commute for each business day, the mobile device usage could shift from the downtown office buildings to the commuter routers and then to the suburban locations. The reverse traffic pattern shift could occur during the morning commute of each business day.

5. Geography and terrain are major factors to both RF propagation and cell tower placement. For example, is the terrain flat and open or is it hilly and tree covered? Does the geography include significant bodies of water?

6. In addition to factors based upon the laws of physics such as those listed above, there are non-technical factors such as zoning, permits, and jurisdictional restrictions which impact the placement and potentially the coverage area of cell towers (e.g., power restrictions).

Consequently, currently deployed Cell Broadcast based geo-targeting will not be consistent across any operator's network or across different operator's networks. The geo-targeting may vary depending on where the alert area happens to be in relationship to the operator's cell towers.

3.3.1.2 Overshooting and Undershooting the Alert Area

Because of RF propagation characteristics, there will be overshoot and undershoot of the desired alert area. This expectation of overshoot and undershoot is true even if only cell towers within the specified alert area broadcast the WEA Alert Message. The size of the overshoot and undershoot cannot be fully predicted as it is dependent on the specified alert

area, the cell tower placements, and the cell tower configurations at the time of the alert.

Another consideration impacting overshooting and undershooting the alert area is how the cell towers are selected for the broadcast of the WEA Alert Message. For example, are only cell towers located within the alert area selected to broadcast WEA Alert Message? Alternatively, are cell towers located within the alert area selected as well on cell towers on the border of the alert area and perhaps "just outside" of the alert area?

3.3.1.3 Geo-targeting Using Only Cell Towers within the Polygon

One option for geo-targeting is to select only the cell towers located within the alert area as shown in the figure below:

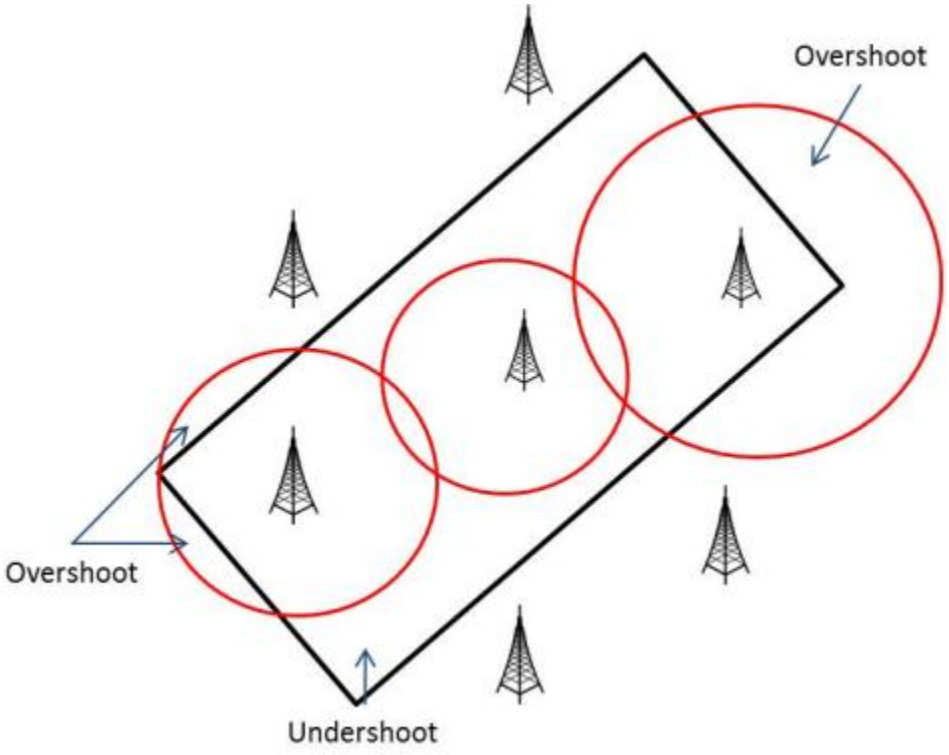


Figure 7: Geo-Targeting With Only Cell Sites Inside Polygon

As shown in the above figure, the selection of cell towers only within the alert area may result in a larger undershoot of the notification to mobile devices within the alert area. The end result of this larger undershoot of WEA Alert Message broadcast is that the WEA Alert Messages may not be received by all potentially reachable individuals within the alert area.

Figure 8 shows the worst case where no broadcasts would occur because there are no cell sites in the alert area.

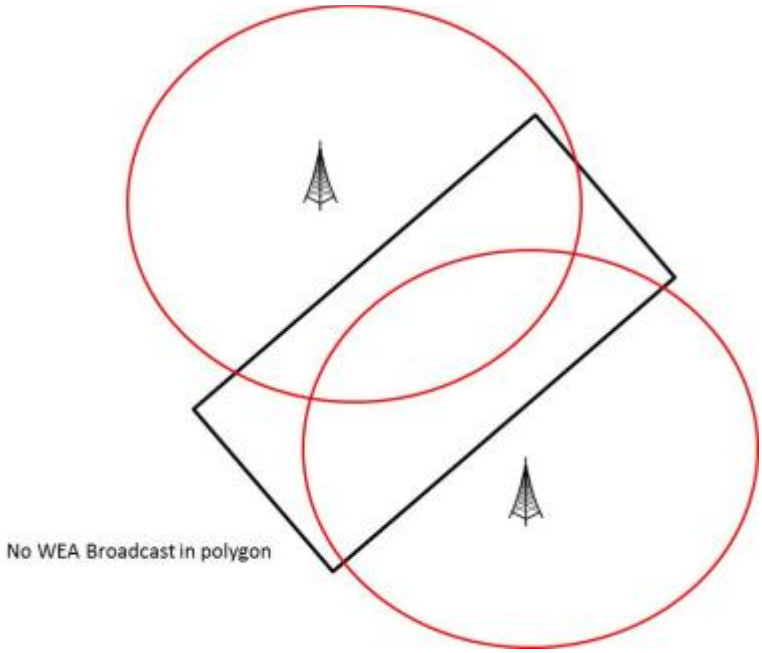


Figure 8: Geo-Targeting With Only Cell Sites Inside Polygon – Worst Case

This worst case scenario could occur under the following types of conditions:

1. In rural areas, because of the low subscriber density and the flat terrain in many rural parts of the country, cell coverage could be provided by cell towers with very large cell radii (e.g., multiple miles). The nickname for this type of cell towers is "boomer" and they could have a cell radius as large as 20 miles or more. Consequently, the cell towers could be many miles apart and it is possible that the alert area polygon could fall entirely between the cell towers as shown in the above figure. Very small alert polygons in rural areas are particularly susceptible to this condition.
2. There are jurisdictions which do not allow for the construction of cell towers within their jurisdictional boundaries. Cell coverage for such jurisdictions is provided by cell towers outside the jurisdictional boundaries with cellular coverage overlapping within the jurisdictional boundaries. If the alert area was the jurisdictional boundary or within the jurisdictional boundary then no cell sites would be selected for the WEA broadcast.

3.3.1.4 Geo-targeting Using Cell Towers Inside and Just outside the Polygon

The amount of undershoot of the alert area might be reduced by using cell towers on the border of the alert area or just outside the alert area in addition to the cell towers within the alert area as shown in the following figure:

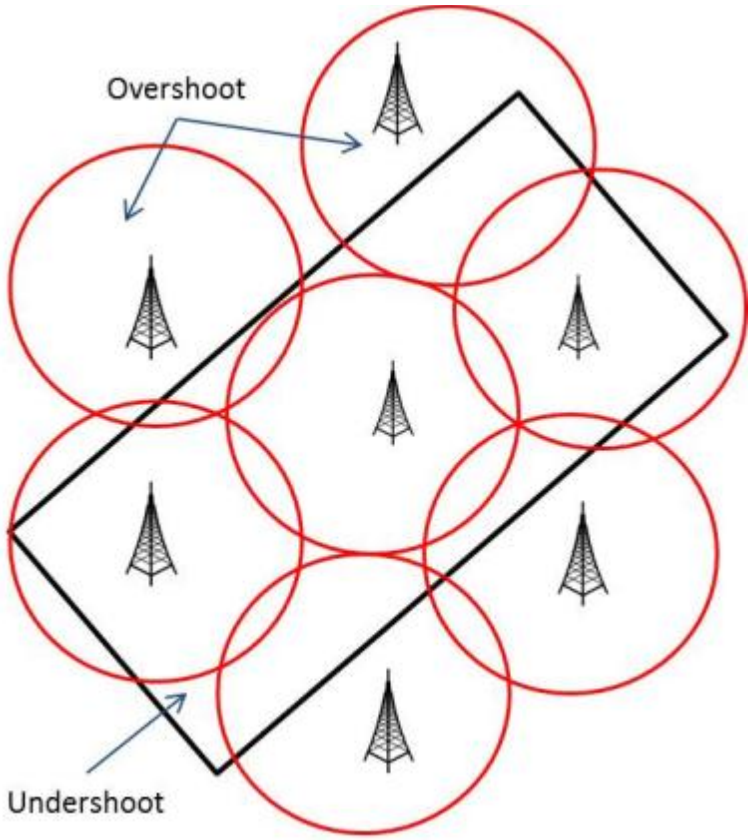


Figure 9: Geo-Targeting With Cell Sites Inside and Just Outside Polygon

As shown in the above figure, the amount of undershoot of coverage within the alert area could be reduced significantly from just using cell sites within the alert area. However, as also shown in the above figure, the possibility of undershooting the alert area still exists.

By utilizing both the cell towers within the alert area as well as cell towers on the boundary or just outside the alert area, the potential of subscribers within the alert area to receive the WEA Alert Message would be maximized. However, there could be a significant increase in the amount of overshooting that occurs. The extent of the overshooting is dependent on the coverage area of the cell towers on the border of the alert area or just outside the alert area. The number of mobile devices outside of the alert area that would receive the WEA Alert Message is currently unpredictable because it is based on cell tower location and characteristics in relation to the alert area.

3.3.1.5 The Geo-targeting Trade-Off

There is a geo-targeting tradeoff that occurs with cell broadcast. The goal is to maximize receipt of the WEA Alert Message by mobile devices within the alert area while minimizing receipt of the alert on mobile devices located outside of the alert area. Cell broadcast based geo-targeting refers to the process of broadcasting the WEA Alert Message from a selected set of radio towers whose collective coverage area is deemed to best approximate the targeted area defined by the Alert Originator. In particular, cell broadcast based geo-targeting does not entail mobile device assistance.

Cell broadcast based geo-targeting constrains the WEA Alert Message broadcast to the best approximation of the alert area given the potential levels of overshoot and undershoot. Due to the underlying CMSP network capabilities, the laws of physics, the impacts of potentially varying geographical, topographical, and environmental conditions (e.g., sunspots, terrain, time of day, airborne particulate matter) and other characteristics of RF propagation, there will not be a 100% match of the RF propagation area and the WEA alert area. Consequently, there will be the potential of "overshoot" and "undershoot" between the WEA alert area and the RF broadcast of the WEA Alert Messages. As part of the trade-off evaluation, the acceptable level of "overshoot" and "undershoot" needs to be considered.

There is no "one size fits all" approach or solution for cell broadcast based geo-targeting. There will always be overshoot and undershoot and the degree of such is not fully predictable and will likely vary among CMSPs.

3.3.2 Issues and Challenges with Current Character Lengths

The CMSAAC report described the technical considerations for the 90 character WEA Alert Message. The CMAS First Report and Order from 2008 says some "commenters raised concerns that a 90 character limit would not provide sufficient information to subscribers about emergencies." Concern about the limitation has been raised by alert originators in multiple forums and through feedback to the Federal government; and has been validated in studies.

In 2010, the Department of Homeland Security Science and Technology Directorate (DHS S&T)[3] sponsored a workshop, titled "Current Knowledge and Research Gaps Workshop on Public Response to Alerts and Warnings on Mobile Devices."[4] The workshop's report concluded that while much information existed on what constitutes effective alert and warning messages, less was known about systems that deliver small amount of information, such as SMS text messages and 90-character WEA Alert Messages. Based on the report's findings and presentations during the workshop, a list of research topics that should be addressed was provided, which included two research topics related to WEA Alert Message length:

- How does a 90-character limit for alerts constrain the ability to provide the public with alerts? What implications does a 90-character limit have on for public response?
- Can such a short message provide enough information to let individuals know that a significant event has taken place? Does it provide enough information for individuals to obtain additional information and take appropriate action to protect themselves?

[3] As detailed in Section 4.2, the WARN tasked DHS S&T to oversee research, development, test and evaluation (RDT&E) activities that address WEA geo-targeting and improve public response.

[4] Workshop was conducted through a contract with the National Academy of Sciences, National Research Council's (NRC's) Committee on Public Response to Alerts and Warnings on Mobile Devices. It was held on April 13 and 14, 2010. The purpose of the workshop was to examine current knowledge and research on how the public responds to alerts and warning with a specific focus on mobile alerting, examine related work on mobile and text messaging, and identify research gaps relevant to the CMAS (WEA) program. DHS S&T had two goals of the workshop: 1) Present what is currently known about public response to alerts and warnings and how that relates to the design, operation, and future development of CMAS (WEA); and 2) identify any gaps in the research.

During 2013 and 2014, DHS S&T funded multiple research projects to address the questions above (among others). The first study is titled "Comprehensive Testing of Imminent Threat Public Messages for Mobile Devices"[5].

Preliminary findings from that study include that short messages offer less to manage public alert and warning response than longer messages; and that shorter messages don't contain enough information to help people overcome pre-conceptions about different hazards based on personal experience, perceived risk, and knowledge, which likely will not match the event they face. (Section 4.2, which provides a summary of DHS studies on mobile alerting, contains additional findings from the report; and Appendix B contains a more detailed report of the findings.)

3.3.3 Issues and Challenges with Current Message Content

The report from the 2010 workshop, "Current Knowledge and Research Gaps Workshop on Public Response to Alerts and Warnings on Mobile Devices" (see Section 3.3.2) notes that a model of an effective alert and warning system should include event detection, message dissemination, message receipt, and response. Box 1, below, provides information gathered from the workshop related to how much information should be included in an alert and/or warning message and what type of content should be included.

[5] This research was supported by the DHS S&T Directorate through Contract Award Number HSHQDC-10-A-BOA36/HSHQDC-12-J-00145 made to the National Consortium for the Study of Terrorism and Responses to Terrorism (START). The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, or START, wireless vendors, wireless network operators, or wireless service providers.

BOX 1

The Warning Process: Message Receipt and Response by the Public

Below is a list of steps that the affected population takes during a crisis or emergency following the receipt of an alert and/or warning message.

- Receive the warning—People must physically receive the warning.
- Understand the warning – Once people receive a warning they must be able to process the message and understand what it means.
- Believe the warning is credible—People must believe that the source of the warning is reliable and the threat could materialize.
- Confirm the threat—People must take steps in order to verify that the threat described in the warning is real.
- Personalize the threat—People must believe that the threat is something that can potentially affect them.
- Determine whether or not protective action is needed—People need to decide if they need to take action.
- Determine whether protective action is feasible—People need to decide if they are able to take action.
- Decide if you have the resources to take protective action—people need to have the resources to actually do what is required.

Thus, the alert recipient must understand the alert, believe it to be credible, have supporting information, and believe the threat is something that can affect them before they will take the prescribed action in the alert.

Additionally, the workshop identified the following list of research topics related to message content that should be addressed:

- What are the message characteristics that lead to effective instruction in crisis situations?
- What does the public want the alert or warning message to say? What do they need to hear?
- To what extent will CMAS (WEA) alerts trigger information-seeking behaviors, and what forms will such behavior take? Might that information-seeking behavior end up leading to the network overloads that CMSAAC voiced concern about?
- To what extent can results of research on social media be applied to gaining an understanding of what the public response to CMAS (WEA) alerts might be?
- How might social media factor into CMAS (WEA) and other official message dissemination?

- How will public education initiatives need to be designed to help?

Preliminary findings from the 2013/2014 "Comprehensive Testing of Imminent Threat Public Messages for Mobile Devices" study (see Section 3.3.2) include:

- The use of acronyms, in place of spelling out words, may limit the effectiveness of the message.
- The phrase "in this area" does not effectively communicate who is at risk. Each WEA that states "in this area" but does not apply to the individual receiving the message may train message receivers that "in this area" may not apply to them.
- The public may not understand terms such as shelter and evacuate.

3.4 Status of Wireless Network Deployment

U.S. wireless carriers continue to tirelessly build out 4G wireless networks, with some having nearly completed their LTE deployment. AT&T Inc. has deployed LTE in more than 500 markets,[6] and its LTE network now covers more than 300 million people.[7] AT&T's 4G LTE build was reported "essentially complete" by the summer 2014.[8] As of January 2014, Sprint had rolled out LTE in 340 markets nationwide,[9] and Sprint's LTE network covered more than 200 million people as of February 2014.[10] Sprint has also announced "Sprint Spark," a tri-band LTE configuration that it plans to deploy in 100 U.S. cities over the next three years.[11] T-Mobile's 4G LTE network covers 250 million people and the company has announced its expectation to expand its coverage to 300 million people in 2015.[12] And Verizon Wireless has implemented LTE in at least 500 markets covering 303 million people (95 percent of the U.S. population),[13] noting that it had "virtually wrapped up its deployment" as of June 2013.[14]

Regional carriers have also aggressively constructed 4G networks. U.S. Cellular, through its partnership with King Street Wireless, now offers 4G LTE service to nearly 90 percent of its

[6] Kevin Fitchard, "AT&T Passes the 500-Market Milestone in its LTE Rollout," Gigaom (Jan. 6, 2014), *at* http://gigaom.com/2014/01/06/att-passes-the-500-market-milestone-in-its-lte-rollout/.
[7] AT&T, "AT&T 4G LTE Network Reaches More Than 300 Million People", at http://about.att.com/story/att_4g_lte_network_expands_reach_to_more_than_300_million_americans.html.
[8] AT&T, "AT&T: The Nation's Most Reliable 4G LTE Network", *at* http://about.att.com/content/dam/snrdocs/4g_evolution_infographic.pdf (last visited March 11, 2014).
[9] News Release, Sprint, "Sprint Rolls Out 4G LTE in More Cities," (Jan. 27, 2014), *available at* http://newsroom.sprint.com/news-releases/sprint-rolls-out-4g-lte-in-more-cities.htm.
[10] News Release, Sprint, "Sprint's All-New Network Brings Sprint Spark and HD Voice to Philadelphia and Baltimore," (Feb. 11, 2014), *available at* http://newsroom.sprint.com/news-releases/sprints-all-new-network-brings-sprint-spark-and-hd-voice-to-philadelphia-and-baltimore.htm.
[11] Sprint, "The All-New Sprint Network," *at* http://network.sprint.com/?ECID=vanity:network (last visited March 11, 2014).
[12] News Release, T-Mobile, "T-Mobile US Reports Third Quarter 2014 Results" (October 27, 2014) available at http://newsroom.t-mobile.com/news/company-news/t-mobile-us-reports-third-quarter-2014-results.htm.
[13] Verizon, "LTE Information Center," *at* http://www.verizonwireless.com/news/LTE/Overview.html (last visited March 11, 2014); News Release, Verizon, "Verizon Wireless Celebrates Three Years (and Counting) of 4G LTE" (Dec. 5, 2013), *available at* http://www.verizonwireless.com/news/article/2013/12/verizon-wireless-4g-lte-three-year-anniversary.html.
[14] Roger Cheng, "Verizon Hits 500 LTE Markets As Focus Shifts to Coverage Over Speed," CNET (June 27, 2013), *at* http://news.cnet.com/8301-1035_3-57591204-94/verizon-hits-500-lte-markets-as-focus-shifts-to-coverage-over-speed/.

customers.[15] Meanwhile, C Spire Wireless has rolled out 4G LTE in 51 Mississippi markets since September 2012, and plans to expand the service to 71 cities and 51 counties covering a population of 496,000.[16] C Spire anticipates that when the latest phase of its deployment is complete in 2014, 6 out of 10 consumers and businesses in Mississippi will have access to its 4G LTE network.[17] Finally, 13 of the 20 participants in Verizon Wireless' LTE in Rural America program have launched their LTE networks. Combined, these networks cover nearly 1.8 million people and more than 41,000 square miles.[18] When all of the LTE in Rural America partners complete their networks, they will cover 2.8 million people and more than 179,000 square miles.[19]

4 Analysis, Findings, and Recommendations

This section provides the analysis, findings, and recommendations for potential enhancements or improvements for the WEA. This section is organized as follows:

- Section 4.1 defines the assumptions and objectives of the subgroup in the development of the analysis, findings, and recommendations.
- Section 4.2 contains a summary of the Department of Homeland Security (DHS) studies on mobile alerting.
- Section 4.3 contains the analysis and findings regarding WEA Alert Message length.
- Section 4.4 provides the analysis and findings on the topic of WEA Alert Message content.
- Section 4.5 summarizes the analysis and findings for geo-targeting of WEA Alert Messages.
- Section 4.6 discusses topics for further study.
- Section 4.7 contains the consolidated set of the subgroup recommendations for potential WEA enhancements and improvements.
- Section 4.8 describes the impact to the WEA standards based upon the subgroup recommendations.

4.1 Assumptions and Objectives for Enhancing WEA

The assumptions and goals for enhancing WEA include the following:

[15] News Release, U.S. Cellular, "U.S. Cellular is Recognized as a J.D. Power 2014 Customer Champion," (March 3, 2014), *available at* http://www.uscellular.com/about/press-room/2014/USCellular-is-Recognized-as-a-JDPower-2014-Customer-Champion.html.
[16] News Release, C Spire Wireless, "C Spire Launches 4G Mobile Broadband Services in Louisville, Mississippi," (Jan. 6, 2014), *available at* http://www.cspire.com/company_info/about/news_detail.jsp?entryId=19100010.
[17] Id.
[18] News Release, Verizon "4G LTE Network Launches in Rural Alaska," (Sept. 4, 2013), *available at* http://www.verizonwireless.com/news/article/2013/09/4g-lte-rural-america-program-alaska.html.
[19] Joan Engebretson, "Thirteenth Verizon Rural LTE Network Turned Up, Courtesy of Matanuska," Telecompetitor (Sept. 5, 2013), *at* http://www.telecompetitor.com/thirteenth-verizon-rural-lte-network-turned-courtesy-matanuska/.

- The goal of enhancing WEA is to make WEA more useful to the public and the Alert Originator community based on:
    - What the industry has learned since WEA was launched in April 2012.
    - The results of WEA research sponsored by the Department of Homeland Security.
    - Design constraints within the end-to-end WEA ecosystem.
- WEA enhancements would have to be developed on an end-to-end basis and must take into account impacts to the A, B, C and D interfaces as well as the hardware and software used to support these interfaces (See Figure 1). In particular, WEA enhancements must not cause or promote network congestion in the wireless network, as there are severe spectrum constraints.
- Legacy LTE handsets as well as 2G and 3G networks/handsets will continue to be capable of the Classic WEA deployed today. Legacy LTE handsets may or may not support enhanced WEA capabilities.
- Enhanced WEA may require that two versions of WEA co-exist for an undetermined period of time. Classic WEA (what is deployed today) must co-exist along with the new and improved enhanced WEA, as described within this report.
- Enhanced WEA features may require the customer to have an enhanced WEA capable mobile device. Enhanced WEA capable mobile devices should be capable of receiving Classic WEA Alert Messages when enhanced WEA is not available.
- Enhanced WEA would continue to be a voluntary election by CMSPs whereby the CMSPs would provide the FCC with their election choice and their implementation timeline for enhanced WEA.

4.2 Summary of DHS Studies on Mobile Alerting

The WARN Act tasked the Department of Homeland Security Science and Technology Directorate (DHS S&T) to partner with academia, the private sector, government labs, and others to perform research, development, test and evaluation (RDT&E) activities that address WEA geo-targeting and improve public response. Accordingly, DHS S&T funded multiple studies in this area. Some of the studies have concluded while others are still underway. Nevertheless, the outcomes from the completed studies underscore the issues and challenges with current WEA character length, content and geo-targeting.

The preliminary findings of the research on “Comprehensive Testing of Imminent Threat Public Messages for Mobile Devices” not only clarify the issues and challenges associated with WEA, but also contain the following findings regarding improvements to WEA:

- Adjusting the order of elements in a 90 or 140 character alert message to source, guidance, hazard, location, and time may improve public response.
- Having a local and recognizable source in the 90-character message may help personalize the message and improve protective action-taking.
- Consideration should be given to discontinue the use of acronyms, educate the public

about their meaning, or increase the message length to allow for full text descriptions.

- The effectiveness of WEA Alert Messages may remain suppressed until they can be distributed to finer geospatial targeted populations so that messages only reach the people who are at risk.
- Inclusion of a map showing the threat area map and the recipient's location helps personalize the threat and could improve protective action-taking. Inclusion of a map without the recipient's location may serve to confuse the recipient.
- Consideration should be given to inclusion of a URL, since there is a long-standing historical observation that people engage in a search for additional information before taking protective action. It remains unclear if inclusion of a URL might reduce or increase the delay in taking a protective action after message receipt.
- WEA Alert Messages should describe basic alert and warning concepts to the extent possible.
- Sound, color, size, shape, and style could all potentially influence WEA Alert Message interpretation and subsequent response but it is not yet known how.

The findings above are consistent with previous studies which conclude that personalizing the threat improves protective action-taking. Appendix B contains a more detailed report of the findings.

4.2.1 Commentary and Improvements Desired by Alert Originators

Alert origination members of the working group most desire that the general public take life-saving decisive action in response to WEA and wish to act on suggestions made by the study.

The study suggests that the alert origination community should help improve WEA in the following ways to better personalize the threat and save lives.

- Optimize the order of WEA Alert Message content. This optimized ordering of the WEA Alert Message content should also consider the CMSAAC report and other studies to reflect the needs of all user communities including individuals with disabilities.
- Incorporate a local and recognizable source in the WEA Alert Message.
- Use the clearest possible language in WEA Alert Messages given message length constraints.
- Use language in the WEA Alert Message that best conveys who is at risk given message length constraints.

The study suggests that improvements to WEA capabilities would enable better personalization of the threat by Alert Originators and help save lives. In line with the results of the study, Alert Originators request that WEA be improved as follows:

- Increase the maximum allowable WEA Alert Message length.
- Distribute WEA Alert Messages to finer geospatial targeted populations so that messages only reach the people who are at risk.

- Include a clickable link that directs WEA recipients to more details about the alert.
- Incorporate an image showing the threat area and the recipient's location. For AMBER Alerts, the image would be of the child and/or abductor. "That would be a huge improvement" according to Robert Hoever, Director of the Missing Children Division at National Center for Missing & Exploited Children.
- Provide a greater range of accessibility for all recipients of WEA Alert Messages, including those who are physically disabled. A separate working group should be established to address accessibility since additional research and expertise by members of the accessibility community is necessary to better understand how sound, color, size, shape, and style could influence WEA Alert Message interpretation.

4.2.2 Commentary by Wireless Industry

While the DHS research does offer some insight into possible enhancements that can improve the recipient's understanding and confidence in the alert message, there is still further research that needs to be performed before final recommendations and standards changes are developed.

The following questions should guide further research:

1. It was mentioned that a "map" gave the recipient of the alert more confidence in the alert message. What would be the impact to the recipient's confidence level in the WEA Alert Message if there was further education/outreach on WEA explaining the purpose and that it comes from a local, trusted source?
2. Has the research looked at all communities of users including individuals with disabilities?
3. There was mention of the "branding" of WEA and that it may not be clear if the displayed message was from a local source or "WEA". If the display screen specifically mentioned the source of the information (i.e., the local agency or NWS) with less or no emphasis on "WEA" branding, would this give the recipient confidence in the WEA Alert Message?
4. The map is used to depict the "in this area" portion of the WEA Alert Message. If WEA is enhanced to allow for 280 displayable characters (subject to technology analysis by ATIS) and can better describe the impacted are, is a map not necessary?
5. The research did not evaluate the actionable points in the WEA Alert Message. What is the impact and user interpretation for all possible actionable instructions that could be in a WEA Alert Message (e.g., shelter in place, take cover now, evacuate, etc.)? There is concern that a map may add confusion for evacuations, shelter in place, etc.
6. What are the potential side effects and potential ancillary consequences (e.g., accident) when trying to read a map to user under all circumstances – driving, etc.?
7. What are the effectiveness and possible consequences if the WEA Alert Message was displayed on the car's dashboard or other vehicle display instead of or in addition to being displayed on the mobile device? Also what would be the effectiveness and possible consequences if text-to-speech is used instead of displaying on the vehicle dashboard or display?

8. What is the impact to mobile device user actions and confidence in WEA and the WEA map if the user location cannot be determined – or if a map is only displayed sometimes (such as when location is available)?
9. A map provides technical challenges. What level of detail is needed on a map and how does the level of detail affect the recipient's understanding and response for both local residents and first time visitors to the alert area indicated on the map?
10. It was mentioned that several of the subjects interpreted the marker on the map as the place they need to travel to in order to shelter in place. How should the maps be formatted so that the marker is clearly understood to be their current location instead of the location they need to travel to?
11. How do the subjects interpret the maps as related to the action in the WEA Alert Message? For example, if the WEA Alert Message indicates "evacuate" do the subjects interpret the map as the location to evacuate from or as the location to evacuate to?
12. How effective are the WEA Alert Messages for the elderly and for individuals with disabilities? For example, if the alert area is provided in only graphical format (e.g., map), how do recipients with vision impairments determine the alert area?
13. If the WEA alert occurs in the middle of the night when the recipients are probably sleeping, would a map or a text based WEA Alert Message be more effective?
14. What is the effectiveness of color on the WEA alert maps to indicate location and polygon including the effectiveness and impact for individuals who are partially or fully color blind?
15. Will the inclusion of clickable URLs in a WEA Alert Message increase or decrease "milling" of users searching for additional internet information related to the alert via their favorite trusted news sources?
16. If it is believed that users will "mill" for internet information after receiving a particular WEA Alert Message regardless of whether a clickable URL is included in the WEA Alert Message, then does it make sense to leave alert area maps to those other news sources?
17. As the WEA alert has a special alert tone or vibration cadence to differentiate these messages from a normal text message or email message, does it make sense to allow users to read these messages while driving (e.g., driving in tornado alley when a tornado alert is issued) even in jurisdictions in which reading text messages is disallowed by law?
18. The research should design experiments that display alert messages on various types of commercially available mobile device screens rather then on computer emulations, in order for users to see the "look and feel" of real devices.
19. The research should explore the user experience in non-"sunny day" scenarios, such as working with CMSPs to understand and emulating real-life impacts of network congestion. This can be emulated in the experiment by introducing delays when clicking on links or browsing for data, not displaying maps due to location not being available, etc.

4.3 Analysis and Findings on WEA Alert Message Length

Consistent with findings from the DHS studies on mobile alerting, that the current maximum 90-character length of WEA Alert Messages constrains public understanding of the messages, Alert Originators have expressed a desire to increase the existing 90-character limit on WEA Alert Message length. There was consensus among the group to recommend the FCC modify their rules to increase the maximum WEA Alert Message length consistent with capabilities of 4G LTE of 280 displayable characters, subject to technology validation by ATIS.

The history of the 90-character WEA Alert Message originates at the CMSAAC with input from a number of consumer stakeholder groups and a desire to have consistency across all CMS technologies. 90 characters was recommended and ultimately adopted by the FCC. From the FCC's First Report & Order for WEA[20]:

> "83. We conclude that, at this initial stage, adoption of a 90 character limit serves the public interest. We agree with commenters such as MetroPCS that a 90 character limit will allow all systems to transmit the message with minimal change, and that 90 characters is an effective limit to allow the message to be delivered and actually be read.[252] As the CMSAAC concluded and the Wireless Rehabilitation Engineering Research Center (WRERC) notes, the 90 character text limit of any CMAS alert is reasonable because the ..CMAS alert is intended to get the attention of a person. The person can then seek out other media for confirmation of the alert and more information.[253]"

As technology advanced from 2G/3G GSM/UMTS/CDMA to the convergence with 4G LTE, the 90 character limit imposed by 2G/3G CMS networks was revisited in this report, and an analysis of impacts to increasing the message length was undertaken. While the desired technology solution for increasing WEA Alert Message lengths is through capabilities of the underlying CMSP infrastructure, other ideas were discussed and summarized in Appendix C. The following table contains a summary of the message length options discussed in Appendix C:

Table 3: Summary of Appendix C Options to Increase Message Length

Appendix Section	Message Option Length Title	Summary
C.1	WEA Alert Message Length Option 1 – Increase Length Using Existing Underlying CMSP Infrastructure Capabilities	This option proposes to increase the maximum length of a WEA Alert Message for LTE beyond the current FCC 90 displayable character rule.
C.2	WEA Alert Message Length Option 2 – Packet-Based Concatenation	This option proposes concatenation of multiple LTE broadcasted packet based messages to assemble the longer WEA Alert Message.
C.3	WEA Alert Message Length Option 3 – Message-Based Concatenation	The wireless carrier transmits the original alert message as a sequence of complete WEA Alert Messages. The WEA OS app is programmed to retrieve that sequence from the WEA inbox, concatenate them, and then present to the end-user.

[20] FCC 08-99, *Federal Communications Commission First Report and Order In the Matter of The Commercial Mobile Alert System*; April 9, 2008.

Appendix Section	Message Option Length Title	Summary
C.4	WEA Alert Message Length Option 4 – Human-Based Concatenation	The original alert message is partitioned into multiple smaller (90 displayable character maximum) alert messages before delivery to the CMSP, adding page numbers to each of the smaller alert messages [e.g., (1/3), (2/3), (3/3)]. Therefore, the original alert message is delivered to the CMSP as multiple individual WEA Alert Messages, and the end-user is relied upon to read them in the correct order.
C.5	WEA Alert Message Length Option 5 – Fewer Bits per Character	Today, the CMSP infrastructure including the radio elements uses an internationally standardized and recognized 7-bits-per-character encoding scheme (3GPP TS 23.038), resulting in a maximum of 630 bits in a 90 displayable character FCC defined WEA Alert Message. It is possible, if defined in global standards, to use alternate character sets that use fewer bits per character.
C.6	WEA Alert Message Length Option 6 – Downloading Over Cellular Connection	Upon receiving the existing 90 displayable character WEA Alert Message, the mobile device can be programmed to treat the cell broadcast reception of a WEA Alert Message as a trigger to fetch more detailed information from a trusted source using the mobile device's cellular data connection.
C.7	WEA Alert Message Length Option 7 – Downloading Over WiFi Connection	Upon receiving the existing 90 displayable character WEA Alert Message, the mobile device can be programmed to treat the cell broadcast reception of a WEA Alert Message as a trigger to fetch more detailed information from a trusted source using the mobile device's WiFi connection (if available).

Option C.1 leverages underlying CMSP Infrastructure capabilities. Options C.2 through C.7 are of varying complexity and potentially greater cost. All options would require varying degrees of further research, technical analysis and industry standardization. The FCC should remain technology neutral and allow technology choices to be decided by Participating CMS Providers and industry standards organizations. As future industry standards evolve which address the number of displayable characters in a WEA Alert Message, the concepts presented in Appendix C should be reviewed.

Taking into consideration the voluntary nature of WEA, CMSP infrastructure technology evolution, market drivers, economic considerations, and handset churn, wireless industry members advise that for legacy 2G/3G CMS networks, there are no practical options to increase the message length beyond the 90 character limit imposed by the underlying CMS infrastructure and deployed technology. Some concepts presented in Appendix C would appear to be applicable to the legacy systems, but those concepts would require feasibility studies, industry standards development, CMS Provider infrastructure and/or mobile device changes (i.e., new mobile devices) which, given the rapid pace of LTE deployments, make retrofitting the legacy systems impractical.

However, 4G LTE, which rapidly has become the predominant technology deployed across nearly all CMSPs, offers the capability to increase the WEA Alert Message length beyond

the 90 character limit of 2G/3G CMS networks. The standards-based LTE technology, with some additional standards and infrastructure implementation changes, supports more than 90 characters and what is likely to be 280 characters as described in option C.1. The term "likely" is used because all LTE page/segment size numbers discussed in this document are subject to review/modifications by national and international standards bodies.

With a displayable character-limit increase for LTE, there will be a requirement for Alert Originators to provide both a 90-character WEA Alert Message to accommodate legacy CMSP infrastructure and mobile devices, and the longer 280-character WEA Alert Message for LTE. Until Alert Originators upgrade their systems, the Alert Originators may only be able to generate 90 displayable character alert messages even on networks supporting enhanced WEA.

Dissemination of multiple alert messages to CMSPs will be required since there will be a mix of capabilities in the deployed base of CMSP infrastructure and mobile devices – some of which would not be technically capable of transmitting/receiving the longer message. The methodology for composing messages should be driven by standards and best practices within the Alert Origination community (including alert origination system software developers), along with FEMA, since the message has to be delivered to the Federal Alert Gateway (using the CAP protocol).

In addition, Participating CMS Providers have to be presented with both a 90 displayable character WEA Alert Message and the longer 280 displayable character WEA Alert Message across the "C" interface. This requires modifications to the following:

- International and joint ATIS/TIA standards
- Federal Alert Gateway
- CMSP Gateway and CMSP infrastructure
- Mobile devices and mobile device behavior

CMSPs in collaboration with alert originators and other stakeholders should identify the maximum practical WEA Alert Message length from a human factor, alerting psychology, and technology capability.

4.4 Analysis and Findings on Message Content

In general terms, a message is a communication of information. Electronic messages may be composed of text, graphics, audio, and/or video content. As described in Section 4.2 *Summary of DHS Studies on Mobile Alerting*, the research results suggest that textual and graphical improvements to WEA would better personalize the alert and save lives. Since the study suggests that further work is necessary to understand how sound would influence WEA interpretation and video was not studied as part of the research, neither audio nor video options will be considered in this document.

4.4.1 Textual WEA Alert Message Content

Textual content improvements to WEA could be accomplished by incorporating the results of

the START study as best practices in the initial and continuing Alert Originator training conducted by FEMA IPAWS. The training would teach Alert Originators how to:

- Optimize the order of WEA Alert Message content.
- Incorporate a local and recognizable source in the WEA Alert Message.
- Use the clearest possible language in WEA Alert Messages.
- Use language in the WEA Alert Message that best conveys who is at risk.

4.4.2 Graphical WEA Alert Message Content

The type of image which would best personalize the WEA, improve public action-taking, and save lives depends on the type of alert. As shown in Figure 10, an image for a weather or evacuation related WEA would show the outline of the defined threat/evacuation area on a map background. As shown in Figure 11, an image for an AMBER Alert WEA would be an image of the abducted child or the abductor. Both figures demonstrate that an adequate image could be achieved in as little as 5 to 10 kB.

Figure 10: Sample GIF image of tornado warning map. Image is 300 x 300 pixels and reduced to 8 colors. Size is 10 kB. Background map from RadarScope app.

Figure 11: Sample JPEG image of abducted child. Image is 148 x 221 pixels and 60% quality. Size is 5 kB. Image from Microsoft Office.

A popular notion is that the image be pushed to the device. However, the maximum packet length for LTE is about 0.3 kB. Thus, numerous packets would have to be broadcast and concatenated on the device in order to achieve a 5 to 10 kB broadcast of the image. Wireless industry advises that since LTE WEA is only designed for text messages, this would be complex and impractical using the existing globally standardized and deployed broadcast technology which uses SystemInformationBlockType12 (SIB12) for WEA [a subset of the global 3GPP Public Warning System (PWS)] on LTE. SIBs are used to broadcast critical system information to ensure proper operation of the overall LTE network. SIB12 is a text only broadcast message that must be kept to a reasonable size to ensure that other more critical SIBs can be broadcasted in a timely fashion. Wireless industry requested that aspects of WEA related to multimedia be deferred to the CSRIC IV WG-2 subgroup on Multimedia.

Alternatives for associating an image with the WEA include a clickable link to an image on an external server, and a device generated map which also shows the recipient's location.

Alternative 1: Clickable Link to an Image on an External Server

In this alternative, the recipient clicks a link below the WEA Alert Message. This opens the device's web browser and displays an image which is hosted on an external server at FEMA IPAWS. FEMA IPAWS would ensure that the file size of the image is less than an agreed upon size, such as 10 kB.

The benefits of this alternative are as follows:

- Alert recipients would be directed to additional information which is lightweight, rather than milling about the web for additional information which may otherwise strain CMSP network resources.
- The link would be considered a vetted, official, trusted source thereby increasing the chances that the public will take appropriate action quickly.

The drawbacks of this alternative are as follows:

- Network congestion leading to network and service degradation may result from a

large number of concurrent point-to-point connections. Thus, subscribers may be currently unable to retrieve the additional information and/or use other services, such as 9-1-1.

- A study would be needed to determine if directing the subscriber to an authoritative source (e.g., "Visit FEMA.gov for more information") or providing a clickable link to lightweight alert information from an authoritative source would decrease or increase congestion compared to the subscriber milling about the web for additional information when no link is provided. The research should also shed light on technical options for mitigating potential network congestion associated with a clickable link.
- **Mobile device behavior:** If clickable URLs are to be added to WEA Alert Messages, then new procedures would need to be developed to describe how the mobile device will handle the presentation of the WEA Alert Message and the content generated by the clickable URL. For example, procedures would need to be developed in standards to describe how the user is able to go back and forth between the WEA Alert Message text and the content generated by the clickable URL to ensure that the WEA Alert Message text does not disappear after the user clicks on the URL (as it would disappear on some current WEA mobile device implementations today). Currently, J-STD-100 (the ATIS/TIA standard for CMAS Mobile Device Behavior)[21] specifies that clickable URLs are not allowed in WEA Alert Messages. If clickable URLs are to be allowed to support enhanced WEA, then J-STD-100 would need to be modified to explain procedures for handling clickable URLs in a user-friendly manner. Message originator considerations must include coordination of WEA alerts and the content of clickable URLs to avoid user confusion. For example, if the content provided by a clickable URL provides updated information related to the alert such that the original alert is effectively rendered obsolete, such updating would need to be explained fully in the content of the clickable URL, i.e., that the clickable URL content may supersede the content of the original alert in some cases. Another message originator consideration is the coordination of WEA Alert Message updates and the content of the clickable URL.
- The subscriber must have a data services plan.
- There would be no way to display the recipient's location with respect to the threat/evacuation area shown in the image, because a simple GIF or JPEG image contains no geo-reference information and FEMA IPAWS would not know the recipient's location. This could be mitigated (since FEMA IPAWS also has the descriptive text that goes along with the alert) by displaying a mobile friendly web page which contains the image and textual details of the alert. 2 kB would allow for a 2,000 character description.

Alternative 2: Device Generated Map with Recipient's Location

Given the expected predominance of LTE over the next few years, as described in the Section 4.3 *Analysis and Findings on WEA Alert* Message Length, the maximum usable LTE packet length of 280 displayable characters is assumed for this alternative. Note that the

[21] J-STD-100, Joint ATIS/TIA CMAS Mobile Device Behavior Specification, January 30, 2009. Available at https://www.atis.org/docstore/default.aspx.

feasibility of supporting 280 displayable characters is subject technology evaluation by ATIS/TIA standards.

In this alternative, the latitude/longitude vertices which define the alert area are broadcast to the device in addition to the standard textual WEA Alert Message. The device uses the vertices to plot an outline of the alert area over a background map which is resident either on the device or in a "Display application" on the device. If the recipient has location services enabled, the recipient's location may also be plotted on the map as shown in Figure 12.

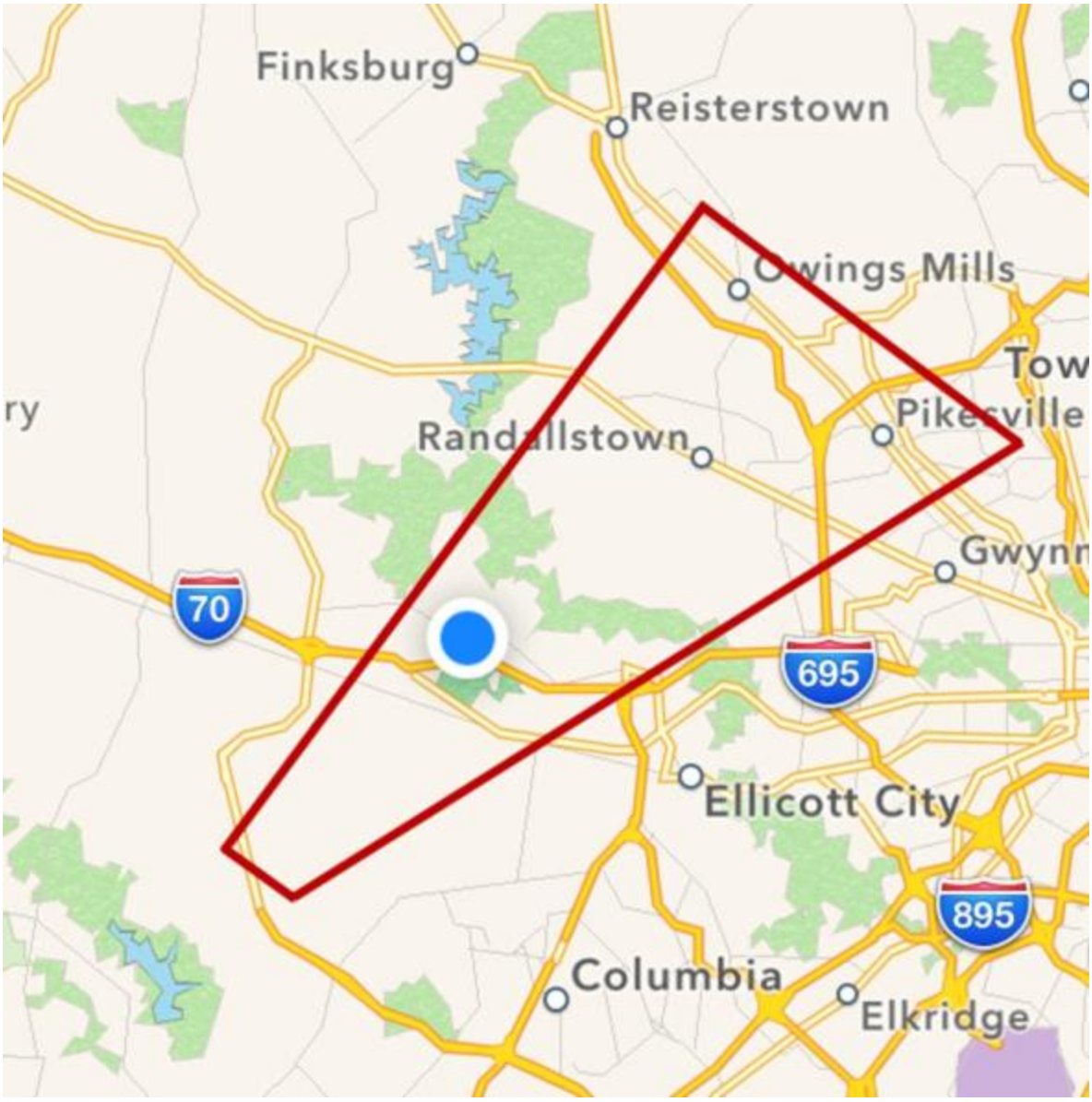


Figure 12: Polygon based warning with the recipients location plotted as a blue and white circle. Map background and recipient location from Apple iPhone Maps.

A standards specification would need to be developed by ATIS/TIA in coordination with FEMA IPAWS (including identification of any Application Programming Interface (API)

needed for a "Display application"). The enhanced WEA capability will be part of the mobile device OS; alternatively the Display app could be developed by third party app developers, in which case a standard API should be made available to app developers. FEMA would develop such a Display app to represent a baseline or "trusted" app among other third party offerings. Consideration should also be given to mobile device users who may choose to download other third party developed Display apps from the appropriate app stores. ATIS/TIA will standardize the enhanced WEA app, the corresponding APIs for the Display app, as well as how the mobile device should behave when enhanced WEA is available and enabled. Activation of the API or enhanced WEA would be subject to CMSP policy.

This alternative results in two messages being pushed via WEA- one for the standard textual WEA displayable message and the second non-displayable message to provide the geocodes (e.g., polygon) to the mobile device. The method will be defined in standards [see Appendix D.5.1 for one example of a method which could be used to package geocodes in an LTE PWS (WEA) broadcast].

The benefits of this alternative are as follows:

- As stated in the START study, a "high information map…specifying the areas affected and not affected and the receiver's location...had a statistically significant and positive effect on public response outcomes including interpretation and personalization".
- The alert recipients would be able to see the image, because little action would be required by the alert recipient to receive it.

The drawbacks of this alternative are as follows:

- This alternative is not possible on non-LTE networks, and further studies need to be made to determine feasibility on LTE networks.
- This alternative may only applicable to smartphones and may not be available on feature phones.
- The recipient's location cannot be plotted if location services are disabled or the device is in a location where location services area unavailable. Also, latency in plotting the device location will result if the device has difficulty establishing the device location.
- Possibility of perceived privacy issue with using the device's location services.
- Use of location services may cause battery drain.
- Use of location services by multiple simultaneous devices could have impact on network resources.
- The subscriber may need a data services plan. Data networks are designed such that the subscriber must have a data service plan to retrieve data.[22]

[22] A Participating CMSP feasibility study would be needed to investigate the ability to access enhanced WEA data from a URL without a data services plan. After the completion of the feasibility study, the FCC may

- The effectiveness is dependent upon the accuracy of the location services.
- Liability and responsibility of the accuracy of the depicted information must be established.

Wireless industry members request that additional social studies be conducted to understand any potential consequences of showing a map to the user, as well as identifying how to tie in the alert text into the map. For example, what does the map indicate and how does it tie into the desired action such as shelter in place/evacuate/etc. Will the map help the user decide what to do, or could it cause further confusion? In regard to this concern, the START study states:

> "The results of the qualitative research indicated that inclusion of a high information map improved most participants' understanding, belief, and risk personalization across all message lengths. These findings suggest that there certainly would be a benefit from adding a high-information map to a WEA Alert Message. Doing so could help the public interpret and personalize the worded message, which could, in turn, move more people at risk to take protective action."

Wireless industry has also raised concern that questions about the meaning of the maps will overwhelm emergency 9-1-1 call center and that CMSP customer care cannot be responsible for answering customer questions or interpreting what the information on a map means. See Section 4.2.2.

The NWS has disseminated polygon based warnings well over 250,000 times since NWS implementation of polygon based warning on October 1, 2007. Those polygons have been viewed many millions of times across a variety of mediums including TV, mobile apps, and other software. While there are no known cases where call centers have been overwhelmed due to display of the polygon, outreach materials provided by WEA partners and stakeholders can be updated to enhance public awareness about the use of polygons. Also, geo-fencing techniques (see Section 4.5 *Analysis and Findings on Geo-Targeting*,) could be employed to mitigate cell broadcast bleedover and limit WEA notification to subscribers in the actual threat area.

4.5 Analysis and Findings on Geo-Targeting

The START study concludes that finer geo-spatial targeting is necessary to ensure WEA Alert Messages only reach those people at risk, otherwise, people who receive WEA Alert Messages may be trained to think they don't apply to them. This section explores various methods which may improve geographic targeting of alert messages, as defined by the alert originator, in order to enhance trust in the alert system, responsiveness to the alerts, and overall public safety.

4.5.1 Current Geographic Targeting

Currently, Participating CMSPs are minimally required to geo-target the WEA broadcast at

choose a policy to require data service at no cost to the subscriber to support retrieval of enhanced WEA information. It is the position of the CMSP operators that a funding source for the retrieval of enhanced WEA information from a URL must be identified.

the county level even if a polygon is defined by the alert originator as the actual alert area. Some CMSPs have voluntarily enhanced WEA in the following ways to geo-target the WEA broadcast to the best approximation of the actual alert area given technology capabilities:

1. Geo-target the broadcast to cell sites approximating the polygon (when a polygon is provided by the alert originator).
2. Broadcast the alert from cell sites based on the overlap of their respective coverage areas with the defined alert area/polygon.
3. Broadcasting alerts to a subset of sectors within a cell to better match the defined alert area/polygon.

These enhancements voluntarily introduced by some Participating CMS Providers have enhanced the geo-targeting to allow best matching of the polygon given the limitations of RF propagation using cell broadcast technology.

4.5.2 Enhancing WEA Geographic Targeting

Section 4.5 and Appendix D focus on technology concepts which might be employed to geographically fence the WEA. Thus, a WEA would only be rendered by devices which are, to the best approximation, within the alert originator's defined alert area. Appendix D.2 details a list of objectives from the Alert Originator's perspective to enhance WEA geo-targeting. While there are feasibility studies required to work out the details, enhanced network-based solutions combined with device centric solutions are recommended for next steps in these studies.

The ideas presented in Appendix D can be generally categorized into:

1. **Device-oriented ideas.** This concept is based on the device filtering which alerts to render by comparing knowledge of its location with the coordinates of the polygon of the target area. As an example, upon receiving an alert the device uses its location-based technology, Standalone GPS or Assisted GPS (A-GPS), to compare its physical location with that of the defined alert area/polygon. If the device determines it is within the polygon and thus meets the defined criteria, the device renders the alert. If the device determines it is outside of the defined criteria, it does not render the alert. The coordinates of the alert area polygon would have to be available to the device. For example, polygon vertices may be broadcasted on the Cellular Broadcast Channel, over a Wi-Fi connection, or a Cellular Data connection. The "defined criteria" for rendering the alert will require standardization for consistency across mobile devices. Ideas to provide the polygon coordinates require further feasibility study.
2. **Optimizations for device-oriented ideas.** The optimizations do not directly enhance geo-targeting, but could enable and/or simplify the implementation of a device-oriented idea. These optimizations would provide alert originators with the ability to deliver more detailed messages (e.g., more displayable characters) and provide the mobile device with the geographic coordinates necessary for device-oriented ideas, while staying within the parameters of today's technology. Such optimizations could include methods to minimize the size of the coordinate data (e.g., through compression of the Geographic Coordinates Data), smoothing of Polygon,

Circularization of Polygon, and Embedding of Geographic Data in the WEA Alert Message. Feasibility study on the optimization ideas is needed.

3. **Network-oriented ideas.** As mentioned earlier, some CMSPs have already made several network-side enhancements to improve WEA geo-targeting such as the implementation of polygon based alerting. Development of an industry best practices specification for geo-targeting in a cell broadcast environment may aid in wider adoption and consistent implementation of these enhancements.
4. **Ideas involving assistance from a third-party** (i.e., a party other than the mobile device and the cellular network). In this idea, a third-party service may be able to determine the location of the mobile device and assist the mobile device in determining if the WEA Alert Message should be rendered.

4.5.3 Summary of Findings

Methods to enhance geographic targeting for WEA Alert Messages using 4G LTE cell broadcast technology have been explored. Based on the START research, these enhancements will assist in personalizing the threat of the message and improve the public's response to alerts. While there are feasibility studies required to work out the details, enhanced network-based solutions combined with device centric solutions are recommended for next steps in these studies.

4.6 Topics for Further Study

This section provides the following list of the topics for further study which have been mentioned or referenced in other sections of this report:

1. Technical confirmation by the ATIS of the 280 displayable character message length for the enhanced WEA Alert Message is needed.
2. A study is needed for the determination of a methodology for choosing transmission sites, based upon existing cell broadcast capabilities, to minimize the overshoot and undershoot of WEA Alert Messages associated with an alert area. The results of this determination will be used for the development of a Joint ATIS/TIA WEA Cell Broadcast Geo-Targeting Best Practices specification. (See Recommendation 3.2 in Section 4.7).
3. A WEA Cell Broadcast Geo-targeting feasibility study is needed to investigate technology enhancements, including mobile-assisted geo-targeting, for enhancing the delivery of alert messages to a given geocode, circle, or polygon. (See Recommendation 3.6 in Section 4.7).
4. An investigation of the needs of individuals with disabilities for enhanced WEA capabilities and WEA Alert Message content is needed. Such an investigation must include the advocates and organizations which represent the community of individuals with disabilities. (See Sections 4.2.1 and 4.2.2).
5. Studies and research to develop responses to the wireless industry questions on DHS research activities as provided in Section 4.2.2 is needed.

6. As stated in Section 4.3, "*varying degrees of further research*" is needed for Options C.1 through C.7 of Appendix C.
7. As stated in alternative #1 in Section 4.4.2:

   "*A study would be needed to determine if directing the subscriber to an authoritative source (e.g., "Visit FEMA.gov for more information") or providing a clickable link to lightweight alert information from an authoritative source would decrease or increase congestion compared to the subscriber milling about the web for additional information when no link is provided. The research should also shed light on technical options for mitigating potential network congestion associated with a clickable link.*"

8. As stated in alternative #2 in Section 4.4.2:

   "*Wireless industry members request that additional social study be conducted to understand any potential consequences of showing a map to the user, as well as identifying how to tie in the alert text into the map. For example, what does the map indicate and how does it tie into the desired action such as shelter in place/evacuate/etc. Will the map help the user decide what to do, or could it cause further confusion?*"

9. As stated in the footnote to alternative #2 in Section 4.4.2:

   "*A Participating CMSP feasibility study would be needed to investigate the ability to access enhanced WEA data from a URL without a data services plan.*"

10. As stated in Recommendation 5.1 of Section 4.7, the development of a Joint ATIS/TIA feasibility study on the standardization/implementation considerations for enhancing a text WEA Alert Message with the following additional information and capabilities is needed:

    a. Display on the device a simple map which shows the threat area and recipient's location in relation to the alert area for imminent threat alerts.
    b. Display on the device a photo such as that of a suspect, missing child, or abductor for Amber Alerts.
    c. Display on the mobile device Hazard symbols (to be defined) associated with a type of event.
    d. Suppression of duplicate alerts when received from multiple sources.
    e. Broadcast of the geocodes (i.e., SAME/FIPS, polygon, or circle coordinates).
    f. Investigate the usage of built-in geo-location and mapping technologies on the mobile handset, taking into account CMSP infrastructure impacts of location determination.
    g. An embedded Uniform Resource Locator (URL) and the impacts to the CMSP network if a large number of users simultaneously access the URL through the cellular data network.

h. Any new long-term technologies, such as enhanced Multimedia Broadcast Multicast Service (eMBMS) for LTE.

i. Usage of alternate data networks (e.g., WiFi, Satellite) when they are available/accessible.

j. Study requirements, use cases, effects, and potential mitigation solutions for making WEA data on the mobile device accessible by trusted developer partners, and address concerns of security, consistency of WEA Alert Messages across CMSPs, devices, and networks as well as CMSP responsibility and support for third party WEA applications.

11. Additional research and feasibility studies are needed for the various geo-targeting concepts presented in Appendix D.
12. Additional research and feasibility studies are needed for the future mobile alert concept in Appendix F. Note: this concept includes use of satellite capabilities and, thus, satellite service providers must be included in these additional research and feasibility study activities.

4.7 Subgroup Recommendations

Note: All references to 280 displayable characters in the Recommendations for Message Length are subject to technology confirmation by ATIS standards. Further research is needed in standards to confirm other technical assumptions in this report.

Technology Neutral and Standards Recommendations

Recommendation 1.1: It is recommended that the Commission remain technology neutral in all rules pertaining to WEA, allowing industry standards to develop and standardize technology for supporting a Participating CMS Provider's WEA obligations.

Recommendation 1.2: It is recommended that prior to the adoption of rules affecting 47 CFR Part 10, the Commission will require any technical standards, protocols, procedures, and related requirements that are adopted be standardized in recognized accredited industry bodies that have well defined Intellectual Property Rights (IPR) policies. Further, consistent with the CMSAAC recommendations, if and insofar as one or more licenses may be required under any of their respective IPR that are technically essential for purposes of implementing or deploying WEA, the rights holders shall license such IPR on a fair, reasonable and nondiscriminatory basis for those limited purposes only.

Recommendation 1.3: It is recommended the Commission recognize that rules are based on current technology capabilities and a joint government-industry partnership should periodically review the capabilities of the technology and recommend further enhancements. The review should occur every three years via the CSRIC structure or in response to major advancements in technology which could improve public safety. Discussion of such technology advancements may occur at the regular WEA partner meetings hosted by the FCC.

Message Length Recommendations

Recommendation 2.1: It is recommended, following technology confirmation by ATIS standards, that 47 CFR § 10.430 Character Limit be modified to such that a WEA Alert Message processed by a Participating CMS Provider has a maximum length of 280 displayable characters of displayable text on capable 4G LTE based CMS Provider Infrastructure and devices. The existing 90 Character Limit rule will remain for 2G, 3G and legacy 4G networks and devices based on the limitations of these networks and the expectation that the overwhelming majority of CMSP infrastructure and mobile devices will churn[23] to capable 4G LTE.

Recommendation 2.2: It is recommended that the industry modify existing CMAS/WEA standards to support coexistence of both the legacy 90 characters of displayable text for use on 2nd and 3rd Generation CMS Provider Infrastructure, and a message length of 280 displayable characters for 4G LTE CMS Provider Infrastructure including the addressing of backward compatibility issues. These standards should support the capability on both the "C" interface and within the CMS Provider infrastructure. It is recommended the standards modifications be complete within one year after the issuance of the FCC Report & Order.

Recommendation 2.3: It is recommended that Participating CMS Provider LTE infrastructure and the FEMA IPAWS Federal Alert Gateway support 280 displayable characters within two years after the completion of the above mentioned industry standards.

Recommendation 2.4: It is recommended that the OASIS CAP v1.2 IPAWS USA Profile V1.0 be modified to support 280 displayable characters limit on message length for enhanced WEA. It is recommended the standards modifications be complete within one year after the issuance of the FCC Report & Order.

Geo-Targeting Recommendations

Recommendation 3.1: It is recommended that 47 CFR 10 § 10.450 Geographic Targeting be modified to state that a Participating CMS Provider may voluntarily transmit any Alert Message that is specified by the Alert Originator using a geocode, circle, or polygon, to an area that best approximates the geocode, circle, or polygon given the constraints of CMS Provider infrastructure topology, propagation area, and other radio and network characteristics. Further, the rules must allow flexibility as Geo-targeting will not be consistent across any operator's network, or across different operators, due to design characteristics and constraints described in this report. If, however, the propagation area of a CMS provider's transmission site exceeds the geocode, circle, or polygon, the FCC rules must allow for a Participating CMS Provider to transmit an Alert Message to an area not exceeding the propagation area of the CMSP transmission site.

> Note: The best approximation of the coverage of the alert area should include as much of the alert area as technically feasible.

[23] In the context of this Recommendation, the term "churn" refers to the wireless subscribers replacing their older technology mobile devices with new technology mobile devices.

Recommendation 3.2: It is recommended that industry, FEMA, and Alert Originators collaborate on the development of a WEA Cell Broadcast Geo-targeting Best Practices Joint ATIS-TIA industry standard describing a methodology for choosing transmission sites in relation to a given geocode, circle, or polygon for transmitting Alert Messages. The WEA Cell Broadcast Geo-targeting Best Practices should leverage the results of research, including the DHS Studies on Geo-targeting which are currently underway.

> Note: This WEA Cell Broadcast Geo-targeting Best Practices should include the evaluation of simple versus complex polygons, number of maximum points in polygon, polygons with crossing lines within the polygon, responsibility for validation of polygons, multiple polygons, multiple circles, and combinations of polygons and circles.

Recommendation 3.3: It is recommended that the WEA Cell Broadcast Geo-targeting Best Practices standard in Recommendation 3.2 be completed within one year after the issuance of the FCC Report & Order, and Participating CMS Providers implement the network based WEA Cell Broadcast Geo-targeting Best Practices standard be completed within two years after the issuance of the FCC Report & Order.

Recommendation 3.4: It is recommended that any Intellectual Property Rights (IPR) issues, which may preclude mobile device geo-filtering of WEA Alert Messages, be addressed by the FCC to allow for enhanced geographic targeting of WEA to the extent that the FCC has any jurisdiction in IPR issues.

Recommendation 3.5: With the major carriers currently supporting Geo-targeting at a sub-county level, it is recommended that Alert Originators be encouraged to provide a polygon or circle when targeting a sub-county area describing the alert area for all WEA Alerts, when operational considerations allow.

> Note: This encouragement should be included in the FEMA provided training on WEA and IPAWS.

Recommendation 3.6: It is recommended that industry, FEMA, and Alert Originators collaborate on an ATIS/TIA feasibility study of WEA Cell Broadcast Geo-targeting. The feasibility study will investigate technology enhancements, including mobile-assisted geo-targeting, for enhancing the delivery of alert messages to a given geocode, circle, or polygon. The WEA Cell Broadcast Geo-targeting feasibility study should leverage the results of research, including the DHS Studies on Geo-targeting which are currently underway. The results of the ATIS/TIA feasibility study will be reported at the regular WEA partner meetings hosted by the FCC-CTIA-DHS-FEMA-NWS-CMSPs.

> Note: This WEA Cell Broadcast Geo-targeting feasibility study should include the evaluation of simple versus complex polygons, number of maximum points in polygon, polygons with crossing lines within the polygon, responsibility for validation of polygons, multiple polygons, multiple circles, and combinations of polygons and circles.

Recommendation 3.7: It is recommended that the WEA Cell Broadcast Geo-targeting feasibility study in Recommendation 3.6 be completed within one year after this recommendation is adopted by the full CSRIC in order to be available for input into the FCC rule making process.

Message Content Recommendations

Recommendation 4.1: It is recommended that further social science studies be conducted to maximize public safety outcomes associated with provision of an image which shows the threat area and recipient's location as well as use of other images such as suspect, abductor/abductee, hazard symbols, etc. It is recommended the studies also compare recipient actions (i.e., "click through" rates where applicable and overall response to WEA) associated with direct provision of an image (e.g., image displayed with WEA Alert Message) versus indirect provision (e.g., recipient must click link or go to secondary application in order to view the image).

Recommendation 4.2: It is recommended FEMA provide training to Alert Originators on incorporating a local and recognizable source in the WEA Alert Message.

Recommendation 4.3: It is recommended FEMA provide training to Alert Originators on using the clearest possible language in WEA Alert Messages given message length constraints.

Recommendation 4.4: It is recommended FEMA provide training to Alert Originators on using language in the WEA Alert Message that best conveys who is at risk given message length constraints.

Recommendation 4.5: It is recommended that FEMA provide training to Alert Originators on any new capabilities which may be deployed as a result of FCC rulemaking following feasibility studies.

Recommendation 4.6: It is further recommended that 47 CFR 10 § 10.440 Embedded Reference Prohibition does not apply for the inclusion of an embedded telephone number for AMBER Alerts.

Recommendation 4.7: It is recommended that the FCC modify the WEA Alert Message Requirements § 10.400 Classification to allow the use of WEA for Emergency Government Information. An Emergency Government Information alert is a message issued by an authorized Federal, State, Tribal, or local government official source to provide essential information directly related to an issued weather or non-weather Imminent Threat Alert. Emergency Government Information is not an alert in itself; it authorizes appropriate agencies the authority to use WEA to provide essential information related to an imminent threat. An Emergency Government Information message should only be used to provide information to assist citizens regarding actions to take resulting from an imminent threat to life and property; information examples are a boil water order, shelter locations, or an extended utility outage notification. The Emergency Government Information should allow for a subscriber opt-out capability (per the WARN Act); this opt-out setting does not imply a new setting, but may be combined with existing settings on the device, to be defined and

specified in the Joint ATIS/TIA mobile Device Behavior Specification.

> Note: The event codes available for use by Emergency Government Information are defined in Appendix C of the National Weather Service Non-Weather Related Emergency Products Specification.[24]

Supplemental Text Feasibility Study Recommendations

Recommendation 5.1: It is recommended that ATIS/TIA perform a study to identify the feasibility and standardization/implementation considerations for supplementing a text WEA Alert Message with additional information requested by Alert Originators in order to maximize public safety outcomes associated with WEA:

- Display on the device a simple map which shows the threat area and recipient's location in relation to the alert area for imminent threat alerts.
- Display on the device a photo such as that of a suspect, missing child, or abductor for Amber Alerts.
- Display on the mobile device Hazard symbols (to be defined) associated with a type of event.
- Providing a method to associate a received WEA Alert Message on the mobile device with the original alert. The use cases for such a method would need to be defined as part of the study, but may include suppressing duplicate alerts (with the goal of not over-alerting) if received from multiple sources including those outside CMSP control, allowing the device/applications to obtain further information from FEMA on the alert, and for the user to seek additional information.

The feasibility study should investigate CMSP infrastructure and mobile device capabilities to identify possible ways to achieve the above capabilities with minimal impacts to CMSP in light of their voluntary election to participate in WEA. Current cell broadcast technology, which is the standardized WEA method used by the major wireless operators, practically cannot support sending multimedia as part of a WEA without significant impacts to CMSP infrastructure. Thus, it is recommended the study consider (but not be limited to):

- A broadcast of the geocodes (i.e., SAME/FIPS, polygon, or circle coordinates) to the device, which most accurately depict the actual alert area, for geographic display of the device's location in relation to the actual alert area, and to determine if the device should display the alert given the location of the device relevant to the actual alert area.
    - This geocode broadcast should also investigate the usage of built-in geo-location and mapping technologies on the mobile handset, taking into account CMSP infrastructure impacts of location determination.
- An embedded Uniform Resource Locator (URL) and the impacts to the CMSP

[24] NWSPD 10-5, *National Weather Service Instruction 10-518, Operations and Services, Public Weather Services, Non-Weather Related Emergency Productions Specification*, August 31, 2013, http://www.nws.noaa.gov/directives/sym/pd01005018curr.pdf.

network if a large number of users simultaneously access the URL through the cellular data network, including recommendations on a "lightweight" content/size.

- Any new long-term technologies, such as enhanced Multimedia Broadcast Multicast Service (eMBMS) for LTE.
- Usage of alternate data networks (e.g., WiFi, Satellite) when they are available/accessible.
- Study requirements, use cases, effects, and potential mitigation solutions for making WEA data on the mobile device accessible by trusted developer partners, and address concerns of security, consistency of WEA Alert Messages across CMSPs, devices, and networks as well as CMSP responsibility and support for third party WEA applications.

The ATIS/TIA feasibility study should include practicality with respect to existing and expected capabilities of CMSP infrastructure, potential IPR issues, evaluation of impacts, and identification of potential solutions that do not unacceptably impact CMSP networks, determination of best possible methodology, standardization timeline, and implementation timelines. In consultation with the Department of Homeland Security Science and Technology Directorate, the study should leverage any relevant social science and mobile alerting related studies.

Recommendation 5.2: It is recommended that the ATIS/TIA feasibility study in Recommendation 5.1 be completed within one year after this recommendation is adopted by the full CSRIC in order to be available for input into the FCC rule making process. The results of the ATIS/TIA feasibility study will be reported at the regular WEA partner meetings hosted by the FCC-CTIA-DHS-FEMA-NWS-CMSPs.

Funding Recommendations

Recommendation 6.1: It is recommended that the FCC identify and establish a method for funding the design, development and deployment of enhancements to WEA recommended in this report and adopted by the Commission through an appropriate rulemaking process.

From the Wireless Industry perspective, Participating CMSPs elected to participate in WEA under the rules developed as a result of the WARN Act and recommendations made to the FCC through the CMSAAC. The WARN Act did not explicitly lay out a continuous series of WEA redesign as part of a Participating CMSPs election. Any proposed enhancements are viewed by the wireless industry as beyond the service envisioned by Congress in enacting the WARN Act, and exceed current CMSP obligations under the Act. Thus, the recommended method for funding the design, development and deployment of enhancements to WEA should apply to Participating CMSPs as well as other stakeholders.

CMS Provider Election & Timeline Recommendations

Recommendation 7.1: It is recommended that the FCC modify the WEA Participation Election Procedures (§ 10.210) to provide an option for Participating CMS Providers to reconfirm their election to support WEA including a process to amend the election to support any modifications or enhancements to WEA rules as adopted by the Commission through an

appropriate rulemaking process. The modified CMS Provider Election Procedures should require a CMS provider to electronically file with the Commission, within 180 days following adoption of changes or enhancements to WEA rules, a letter attesting that the Provider either:

A. Elects to maintain the CMS Provider decision not to participate in WEA or withdraws its election to no longer continue to participate in WEA (subject to § 10.220, Withdrawal of Election to Participate in WEA); or
B. Elects to continue participation based on the CMS Provider's original election to participate under the rules in place at the time of the original election; or
C. Elects to participate in whole or in part with the modified or enhanced WEA rules and:
    1. Agrees to transmit such alerts in a manner consistent with the enhanced WEA technical standards, protocols, procedures, and other technical requirements for enhanced WEA implemented by the Commission and standardized in an appropriate industry standards body;
    2. Commits to support the development and deployment of technology for the enhancements to the "C" interface, the CMS provider Gateway, the CMS provider infrastructure, and mobile devices with enhanced WEA functionality;
    3. Supports the CMS provider selected technology to meet obligations under (1) and (2).

Discussion: The initial deployment of WEA required significant unfunded investment by CMSPs. There is concern that some CMSPs, especially smaller/rural carriers which elected to participate in WEA under the existing rules, did not anticipate continuous changes to WEA and thus may not be able to support another unfunded investment to upgrade to support any enhancement. If the expectation is to upgrade the network infrastructure to support enhancements to WEA, some operators may choose to withdraw their election to participate in WEA because their business models cannot support such infrastructure upgrades. Option "B" is to provide those operators which are currently participating in WEA the ability to continue to participate with their current investments in infrastructure under the existing rules. The intent is to avoid the scenario where a CMSP withdraws from WEA because their business model will not support the enhancements, so rather than withdrawing their election, this allows them to continue to participate with the current WEA so their subscribers at least get the WEA capabilities they have today.

Recommendation 7.2: It is recommended that within 180 days of the FCC adoption of rules for WEA enhancements, the FCC, Participating CMS providers, FEMA, and Alert Originators jointly identify the timelines for enhanced WEA development, testing and deployment, including the FEMA timeline for support of enhanced WEA in the Federal Alert Aggregator and Alert Gateway. The timeline should also take into consideration completion of industry feasibility studies and establishment of industry standards development timelines.

4.8 Impact to Standards

In order to support the recommendation for 280 displayable characters of displayable text in LTE, a number of existing standards may need to be modified in both North American and Global standards. These standards include but not limited to:

ATIS-0700008 .....Cell Broadcast Entity (CBE) to Cell Broadcast Center (CBC) Interface Specification

ATIS-0700010* .....CMAS via EPS Public Warning System Specification

ATIS-0700014 .....Implementation Guidelines for CMAS Handling of CMAS Supplemental Information Broadcast

J-STD-100*.....Joint ATIS/TIA CMAS Mobile Device Behavior Specification

J-STD-101.....Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification

J-STD-102*.....Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Test Specification

3GPP TS 23.041.....3GPP Technical realization of Cell Broadcast Service (CBS)

OASIS CAP v1.2 .....IPAWS Profile for the OASIS Common Alerting Protocol IPAWS USA Profile V1.0

* These standards have Supplements.

Note that other recommendations will have additional impact to the standards that must be identified by ATIS/TIA during the feasibility study.

5 Conclusions

WEA is recognized as an important public safety tool. It is one of the many tools that make up this nation's larger warning system. Enhancements to increase the effectiveness of WEA and overall public safety are recognized by all stakeholders. The working group's effort focused on recommending enhancements to WEA which are based on needs expressed by alert origination members of the working group and are technically feasible as a voluntary service by Participating CMS Providers.

Participating CMSPs expressed that any enhancements be technologically neutral without harming commercial wireless networks and service to their subscribers. Members of the alert origination community desire improvements which would personalize the threat and improve public response to WEA Alert Messages based on outcomes from social science studies and long known tenets of public alerting.

Based on input from all stakeholders, there was consensus among the group to submit the recommendations in Section 4.7 for consideration by the FCC and industry. Obtaining consensus on supplementing the WEA with graphical information and enhancements to geographical targeting was more challenging. Thus, an ATIS/TIA feasibility study is recommended. The study would consider several alternatives, potential impacts to CMSP networks, and be completed in time to be available as input to the FCC rule making process.

Appendix A: Existing WEA Standards

CMAS implementation in the United States has been based on industry standards. ATIS, TIA, and Joint ATIS/TIA standards for CMAS were developed based on cell broadcast and Public Warning System (PWS) specifications in 3GPP and 3GPP2. The following table is a listing of the major CMAS-related standards (as well as some related FCC docs and the WARN Act) used to support implementation of Wireless Emergency Alerts (WEA) in the United States.

Table 4: Existing WEA Standards

Number	Title	Description
ATIS-0700006	CMAS via GSM/UMTS Cell Broadcast Service Specification	This ATIS specification defines the requirements, architecture, interfaces, call flows, and message formatting for the support of CMAS on the GSM Cell Broadcast Service.
ATIS-0700006.a	Supplement A to ATIS-0700006, CMAS via GSM/UMTS Cell Broadcast Service Specification	This supplement provides errata and clarifications to the published version of ATIS-0700006, CMAS via GSM/UMTS Cell Broadcast Service Specification.
ATIS-0700007	Implementation Guidelines and Best Practices for GSM/UMTS Cell Broadcast Service	This ATIS specification provides implementation guidelines and best practices for the implementation of CMAS on the GSM Cell Broadcast Service. Detailed call flows regarding the behavior of CMAS on the air interface is included in this specification.
ATIS-0700008	Cell Broadcast Entity (CBE) to Cell Broadcast Center (CBC) Interface Specification	This ATIS specification defines an interface and message format for Cell Broadcast messages from the Cell Broadcast Entity (CBE) to the Cell Broadcast Center (CBC). The 3GPP specifications do not define this interface. The CBE is the entity which creates the Cell Broadcast messages for broadcast by the CBC. In CMAS, the CMSP Alert Gateway is the CBE.
ATIS-0700010	CMAS via EPS Public Warning System Specification	This ATIS specification defines who CMAS is supported in the LTE environment since Cell Broadcast does not exist in the LTE environment. This ATIS specification defines the requirements, architecture, interfaces, call flows, and message formatting for the support of CMAS on LTE.
ATIS-0700010.a	Supplement A to ATIS-0700010, CMAS via EPS Public Warning System Specification	This supplement provides errata and clarifications to the published version of ATIS-0700010, CMAS via EPS Public Warning System Specification.
ATIS-0700012	Implementation Guidelines for CMAS Supplemental Information Retrieval	This ATIS specification defines how the CMAS Alert Gateway could retrieve CMAS Supplemental Information from the Federal Alert Gateway. The primary supplemental information is the alert message in Spanish. As of November 2013, FEMA has not agreed to implement this specification.

Number	Title	Description
ATIS-0700013	Implementation Guidelines for Mobile Device Support of Multi-Language CMAS	This ATIS specification defines the guidelines for mobile devices which support CMAS in multiple languages (e.g., English & Spanish). This specification applies to GSM, UMTS, and LTE. This specification is also applicable in the international environment. This specification will be applicable whenever CMAS in Spanish is implemented.
ATIS-0700014	Implementation Guidelines for CMAS Handling of CMAS Supplemental Information Broadcast	This ATIS specification describes the functionality of Cell Broadcast based CMAS when the CMAS messages are being broadcast in both two languages (e.g., English and Spanish). This specification will be applicable whenever CMAS in Spanish is implemented.
J-STD-100	Joint ATIS/TIA CMAS Mobile Device Behavior Specification	This Joint ATIS/TIA specification defines the behavior of the mobile device when it receives a CMAS message.
J-STD-100.a	Supplement A to J-STD-100, Joint ATIS/TIA CMAS Mobile Device Behavior Specification	This supplement provides errata and clarifications to the published version of J-STD-100, Joint ATIS/TIA CMAS Mobile Device Behavior Specification. This specification applies to both 3G and 4G.
J-STD-101	Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification	This Joint ATIS/TIA specification defines the interface between the Federal Alert Gateway and the CMSP Alert Gateway. This interface is commonly called the "C Interface" because of its location on the architecture diagram (see Figure 1).
J-STD-101.a	Supplement A of J-STD-101, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification	The FCC 2nd Report and Order on CMAS defines an optional method for the distribution of CMAS messages from the Federal Alert Gateway to the CMSP Alert Gateway via the Public Television broadcast network. This supplement defines the C Interface Over The Air (C-OTA) from the Public Television Digital Television (DTV) Receiver and Decoder to the CMSP Gateway. There are no known implementations of this capability.
J-STD-101.b	Supplement B of J-STD-101, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification	This supplement provides errata and clarifications to the published version of J-STD-101, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification.
J-STD-102	Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Test Specification	This Joint ATIS/TIA specification defines the test environment and test cases to test the interface between the Federal Alert Gateway and the CMSP Alert Gateway. This interface is commonly called the "C Interface" because of its location on the architecture diagram.
J-STD-102.a	Supplement A of J-STD-102, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Test Specification	This supplement provides errata and clarifications to the published version of J-STD-102, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Test Specification.

Number	Title	Description
TIA-637-D	Short Message Service (SMS) For Wideband Spread Spectrum Systems	These technical requirements form a specification for SMS, providing delivery of text and numeric information for paging, messaging and voice mail notification for SMS over CDMA Systems.
TIA-1149	Commercial Mobile Alert Service (CMAS) over CDMA Systems	The standard covers support for Commercial Mobile Alert Service (CMAS). The network entities and associated reference points that comprise the CMAS Reference Architecture for CDMA are included. This standard provides a specification for CMAS over CDMA Systems.
TIA/EIA/IS-824	Generic Broadcast Teleservice Transport Capability - Network Perspective	This Telecommunications Industry Association (TIA) standard provides a specification for the broadcast capability used in CDMA systems.
3GPP2 S.R0030-A	Broadcast/Multicast Services – Stage 1 Revision A	This document defines the functional characteristics and requirements of Broadcast/Multicast Services.
3GPP2 C.S0077-0	Broadcast Multicast Service for CDMA2000 1x Systems	This document defines requirements for support of the Broadcast/Multicast Service (BCMCS) capability on cdma2000® 1x spread spectrum systems.
3GPP2 X.S0022-A	Broadcast and Multicast Service for cdma2000 Wireless IP Network	This document defines core network protocols and procedures for support of the Broadcast-Multicast Service (BCMCS) for cdma2000® networks.
3GPP TS 22.268	PWS Requirements	This 3GPP document provides the stage 1 requirements for Public Warning System (PWS). WEA is a part of PWS.
3GPP TS 23.041	3GPP Technical realization of Cell Broadcast Service (CBS) (Release 12)	This 3GPP specification for Cell Broadcast service includes the global requirements for the Commercial Mobile Alert Service (CMAS) and the Japanese Earthquake and Tsunami Warning System (ETWS).
3GPP TS 25.419	UTRAN Iu-BC Interface: Service Area Broadcast Protocol (SABP)	This 3GPP document specifies the *Service Area Broadcast Protocol (SABP)* between the Cell Broadcast Centre (CBC) and the Radio Network Controller (RNC).
3GPP TS 23.038	Alphabets and language-specific information	This 3GPP document defines the character sets, languages and message handling requirements for SMS, CBS and USSD.
3GPP TS 23.401	General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access	This 3GPP specification defines the Stage 2 architectural service description for the Evolved 3GPP Packet Switched Domain - also known as the Evolved Packet System (EPS). The Evolved 3GPP Packet Switched Domain provides IP connectivity using the Evolved Universal Terrestrial Radio Access Network (E-UTRAN). The specification covers both roaming and non-roaming scenarios.
3GPP TS 25.324	RAN Broadcast/Multicast Control (BMC)	This 3GPP document provides the description of the Broadcast/Multicast Control Protocol (BMC). This protocol adapts broadcast and multicast services on the radio interface.

Number	Title	Description
3GPP TR 25.925	Radio Interface for Broadcast/Multicast Services	This 3GPP document provides a general overview on radio interface related aspects of broadcast/multicast services. This report covers stage 2 and stage 3 aspects of the radio interface.
3GPP TS 29.168	Cell Broadcast Centre interfaces with the Evolved Packet Core; Stage 3	This 3GPP document describes the procedures and protocols used on the interface between the Mobility Management Entity (MME) and the Cell Broadcast Center (CBC).
3GPP TS 36.300	EUTRAN: Overall Description, Stage 2	From a WEA point of view, this 3GPP document describes the interface between MME and eNB at a stage 2 level.
3GPP TS 36.331	Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification	This 3GPP document specifies the Radio Resource Control protocol for the UE-E-UTRAN radio interface.
3GPP TS 36.413	EUTRAN S1 Application Protocol; stage 3	From a WEA point of view, this 3GPP document describes the interface between the MME and the eNB.
3GPP TS 44.012	Short Message Service Cell Broadcast (SMSCB)support on the mobile radio interface	This document provides radio support for SMSCB, a service in which short messages may be broadcast from a PLMN to Mobile Stations (MS)s.
3GPP TS 48.049	BSC-CBC Interface Specification for CBS	This 3GPP document defines the interface specification for CBC to BSC communication to support CBS.
3GPP TS 48.058	BSC to BTS Interface Specification: layer 3	This 3GPP document defines the layer 3 details of BSC to BTS interface.
OASIS Common Alerting Protocol (CAP)	Alert Originator to Federal Alert Gateway Application Protocol	The Common Alerting Protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks.
OASIS CAP v1.2 IPAWS USA Profile V1.0	Common Alerting Protocol, V. 1.2 USA Integrated Public Alert and Warning System Profile Version 1.0	This OASIS document describes an interpretation of the OASIS CAP v1.2 standard necessary to meet the needs of the Integrated Public Alert and Warning System (IPAWS), a public alerting "system of systems" created by the U.S. Federal Emergency Management Agency.

Appendix B: Findings and Recommendations from the DHS Studies on Mobile Alerting

The U.S. Department of Homeland Security (DHS) is committed to using cutting-edge technologies and scientific talent in its quest to make America safer. The Department of Homeland Security Science and Technology Directorate (DHS S&T) is tasked with researching and organizing the scientific, engineering, and technological resources of the United States and leveraging these existing resources into technological tools to help protect the homeland.

DHS S&T established the Commercial Mobile Alert Service (CMAS) [now referred to as Wireless Emergency Alerts (WEA)] research, development, testing and evaluation (RDT&E) program to develop a collaborative, information technology laboratory capability that facilitates systems research, technology development, and testing and evaluation related to public alerts and warnings. The WEA RDT&E program faces the organizational challenge of aligning the efforts of a diverse research community in the public and private sectors to specific legislative mandates and national goals.

The RDT&E program is enabling and enhancing a national capability to deliver geographically-targeted alert messages to mobile devices and pagers that elicit the intended public response. Per the Warning, Alert, and Response Network (WARN) Act, DHS S&T will partner with academic institutions, the private sector, government laboratories, and other entities to perform RDT&E activities that address geo-targeting and public response capability gaps.

DHS S&T has established the National Consortium for the Study of Terrorism (the START Center) at the College of Behavioral and Social Science, University of Maryland at College Park as a Center of Excellence (COE). As outlined in START's statement of work (SOW), the START Center will conduct a public response-related project entitled, "Comprehensive Testing of Imminent Threat Public Messages for Mobile Devices."

A preliminary report of START's research findings were delivered to the DHS Science and Technology Directorate in January 2014.

The authors of that document are Hamilton Bean, Assistant Professor at the University of Colorado, Denver; Michele Wood, Assistant Professor at California State University, Fullerton; Dennis Mileti, Professor Emeritus at University of Colorado, Boulder; Brooke Liu, Associate Professor at University of Maryland, College Park; Jeannette Sutton, Senior Research Associate at Trauma Health and Hazards Center at the University of Colorado, Colorado Springs; and Stephanie Madden, Doctoral Fellow at the University of Maryland, College Park. Questions about this document should be directed to Dr. Bean at hamilton.bean@ucdenver.edu and/or Dr. Wood at mwood@fullerton.edu.

This research was supported by the Science and Technology Directorate of the U.S. Department of Homeland Security through Contract Award Number HSHQDC-10-A-BOA36/HSHQDC-12-J-00145 made to the National Consortium for the Study of Terrorism and Responses to Terrorism (START). The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing

the official policies, either expressed or implied, of the U.S. Department of Homeland Security, or START, wireless vendors, wireless network operators, or wireless service providers.

Below are primary conclusions extracted from the Report's Executive Summary and represent the research performed to date are:

1. Short alert and warning messages (90- and 140-characters) are unique and unlike any others: The optimized order of their contents is unique; their limited length constrains public understanding of the message source; people are less able to understand if the message is meant for them; the key content elements of guidance (describing what to do and how to do it) and hazard (describing why they should do it) cannot be adequately communicated; and short messages cannot overcome people's pre-event hazard-specific perceptions. Hence, to be effective at motivating public protective action taking, the short messages in use today rely on information provided by others.
2. There are pathways forward to optimize today's wireless emergency alert messages: An alternative order of message contents could be put into practice; message sources of a particular kind could be selected; and a public education and marketing campaign about the WEA system could be conducted.
3. The project's findings provide concrete insights to help imagine optimized wireless emergency alert and warning messages that could exist in the future. These messages would not rely on information provided by others, but would instead be sufficient to motivate public protective action taking on their own. In addition to putting into practice an alternative order of message contents, selecting message sources of a particular kind, and conducting a public education and marketing campaign about the WEA system, the optimized messages of the future could also include high information maps, and allow for up to 1,380-characters message in length.

Key findings from the research reported here suggest that:

4. Order of Message Contents. **A different order for the content contained in 90-characters WEA messages may improve public response outcomes.** WEA messages currently use the following order: hazard, location, time, guidance, and source. An alternative order had an advantage in improving the public outcomes tested. It was: source, guidance, hazard, location, and time. Although this alternative order only had a statistically weak advantage over the current WEA message content order, if put into practice, the effect of the revised order could be substantial considering how many more people in a population at risk might be inclined to take action in response to the revised order. The qualitative research provided support this optimized message order for 140-characters messages; however, it does not appear to transfer to 1,380-characters messages for which the optimized order seems to be source, hazard, guidance, location, and time.
5. Message Source. **Source in 90-characters messages had a statistically significant effect on some sense making public response outcomes including interpretation (understanding, believing, and deciding) and personalization, and, hence, likely on protective action-taking.** Quantitative and qualitative findings also suggest that local and recognizable sources might be the most productive sole source to name in a

WEA message, but further research is needed to confirm these unstable conclusions. Findings here, however, do more conclusively suggest that if a sole source named in a WEA message is not recognizable to the public (e.g., WEA), then a vigorous public education and marketing campaign would be worthwhile. Quantitative findings also suggest that there may not be a single sole source that works for all WEA messages. The same conclusions were reached based on qualitative investigations of 140- and 1,380-characters messages.

6. Map Inclusion. **High information map inclusion (specifying the areas affected and not affected and the receiver's location) in 90-characters messages had a statistically significant and positive effect on public response outcomes including interpretation and personalization, and, hence, could have a positive effect on protective action-taking.** Inclusion of a low information map (specifying the areas affected and not affected, but not the receiver's location) had the opposite effect. The results of the qualitative research indicated that inclusion of a high information map improved most participants' understanding, belief, and risk personalization across all message lengths. These findings suggest that there certainly would be a benefit from adding a high-information map to a WEA message. Doing so could help the public interpret and personalize the worded message, which could, in turn, move more people at risk to take protective action.

7. Relative Importance of Contents Elements. **Guidance and hazard message content elements played key roles compared to other message content elements (location, time, and source) in facilitating the sense making outcomes of interpretation (understanding, believing, and deciding) and personalization. They also reduced milling (causing delay in taking a protective action). Hence, they have a positive effect on public alert and warning responses.** The additional quantitative and qualitative findings affirm and provide a possible explanation for these findings: Perhaps placing guidance and hazard up front in a 90-characters WEA message optimized outcomes because they are the most important content elements. These findings suggest that the *core content of a public alert and warning: Tell people exactly what to do (guidance) and describe why they should do it (hazard).* Those who prepare future public alert and warning messages might consider emphasizing these content topics, but not to the exclusion of the others.

8. Generalizing Across Hazard Types. **Short 90- and 140-characters messages were substantially less effective than 1,380-characters messages at helping people overcome their pre-conceived perceptions about different hazards and likely would be less effective at guiding people to take protective actions appropriate to the risk they face in an actual event.** In this study, the content elements of 1,380-characters messages delivered over mobile communication devices have standardized effects on outcomes regardless of hazard type (generalize across hazards). However, 90- and 140- characters messages did not. Shorter messages do not appear to contain sufficient information to help people overcome their pre-conceptions about different hazards based on their personal experience, perceived risk, and knowledge, which likely will not match the event they face. Hence, short messages appear to offer substantially less to effectively manage public alert and warning response than longer messages.

9. Message Length Efficacy. **The scientific evidence assembled led to the conclusion**

that messages that are 1,380-characters appear to produce optimized interpretation, personalization and milling outcomes, and would likely yield maximized public protective action-taking behavior. Shorter messages that are 90- and 140-chracters appear less effective at guiding people toward protective action taking. There is nothing inherently better about 1,380-characters messages. What is likely the case is that people need to be provided with sufficiently detailed information about exactly what steps to take to protect themselves, and the number of characters needed to accomplish this likely varies across hazards. **Participant and professional emergency manager opinions, however, led to the conclusion that 140-charactres messages were the most desirable. This reveals what may be an American alert and warning dilemma: Should alert and warning message lengths be based on knowledge gained by application of the scientific method, or on beliefs and opinion?**

10. Inclusion of a URL. **Consideration should be given to including a URL in wireless emergency alert and warning messages of any message length.** Doing so would be consistent with the long-standing historical observation that people who are warned engage in a search for additional information before taking a protective action. It remains unclear, however, if inclusion of a URL in alerts and warnings might reduce or increase the delay in taking a protective action after message receipt.

11. Familiarity with the WEA System. **There is a lack of public familiarity with the WEA system.** One might hypothesize that this lack of familiarity would play a role in the effectiveness of the system when in use. **If it is determined that prior familiarity with the WEA system improves public response, then a campaign to educate the public about the WEA system would be appropriate.**

12. Understanding of Acronyms. **The public may have little or no understanding of the acronyms used in WEA messages. Hence, consideration should be given to modifying the system to discontinue the use of acronyms, educate the public about their meaning, or increase the message length to allow for full text descriptions rather than acronyms.** There may be unique exceptions. For example, it is likely that in tornado alley, members of the public are well aware than NWS represents the National Weather Service.

13. How to Best Express Time. **The way WEA messages express time may confuse the public.** Currently, WEA messages express time by stating when the message expires so that such messages do not persist in perpetuity. This serves an important function, but also confuses the public and may delay protective action taking. If time is expressed in WEA messages with language about the time a message expires, **consideration also should be given to communicating the time a message "begins" (without increasing message length) to reduce public confusion. For example, if the words "now" or "immediately" are used, would capitalizing all the letters in those words help to communicate that the message is already in effect when people receive it?**

14. How to Best Express Location. Given the 90-character limit of current WEA messages, **the phrase "in this area" does not effectively work to communicate who is and who is not located within the risk area.** Each WEA disseminated message that states "in this area" but does not apply to the individual receiving the

message may train message receivers that the phrase "in this area" may not apply to them. **The effectiveness of current WEA messages may remain suppressed until they can be distributed to finer geospatial targeted populations so that messages only reach the people who are at risk. We do not yet know how to best communicate in a WEA message who is and who is not at risk, for example, by including impact area maps, finer grained distribution, or the use of longer text messages that allow description of the risk area.**

15. Optimum Level of Fear Arousal. Alert and warning messages elicit a wide range of varied emotional responses. However, the impact fear and other emotions on public alert and warning response could not yet be clarified based on the experimental and focus group methods used to date. **The precise roles emotions may play in making sense of and responding to public alert and warning messages remains unknown, but it will be investigated in the project's research where the emotion to response relationship can be assessed**. If a relationship between emotional response and alert and warning message response is established, then the role of message attributes on emotional outcomes should be examined and taken into account.

16. Understanding of Alert and Warning Concepts. **The public may not understand basic alert and warning concepts. Messages should not rely on the assumption that the public understands terms such as *shelter* and *evacuate*.** Alert and warning messages that are short and contain concepts such as *shelter* and *evacuate* may mean different things to different people who receive the message. For example, the standard *evacuate to higher ground* tsunami message may mean twenty feet above sea level to some, and one hundred feet above sea level to others. Short 90- and 140-characters messages are, therefore, not likely to maximize public health and safety in rapid onset events such as a poison gas release in a subway, a locally generated tsunami, and more. **For messages that are longer than 90- and 140-characters, basic alert and warning concepts should be described to the extent possible.** Short 90- and 140-characters messages may work fine for events whose impact is not imminent.

17. Visualization. Visual stimuli including bullets, bolding, iconography (source logo/seal, for example), indentation, font size, color, or italics, etc. might influence WEA message interpretation and subsequent message response. Additionally, so might the character of audible tones that indicate the arrival of a message. **Sound, color, size, shape, and style could all potentially influence WEA message interpretation and subsequent response but it is not yet know how.**

Appendix C: Alternatives for WEA Alert Message Length Options

This Appendix describes the following WEA Alert Message length options considered by the subworking group:

- WEA Alert Message Length Option 1 – Increase Length Using Existing Underlying CMSP Infrastructure
- WEA Alert Message Length Option 2 – Packet-Based Concatenation
- WEA Alert Message Length Option 3 – Message-Based Concatenation
- WEA Alert Message Length Option 4 – Human-Based Concatenation
- WEA Alert Message Length Option 5 – Fewer Bits per Character
- WEA Alert Message Length Option 6 – Downloading Over Cellular Connection
- WEA Alert Message Length Option 7 – Downloading Over WiFi Connection

All specific LTE-supported maximum message lengths and LTE page/segment size numbers mentioned in this document are subject to review/modification by national and international standards bodies. The potential WEA Alert Message lengths to be supported by LTE throughout this document are examples, and the actual numbers will depend on operator implementation decisions.

C.1. WEA Alert Message Length Option 1 – Increase Length Using Existing Underlying CMSP Infrastructure Capabilities

Even though GSM, UMTS & LTE can transmit more than 90 displayable characters in a cell broadcast message, and some CDMA systems can transmit more than 90 displayable characters in a cell broadcast message, this option proposes to increase the maximum length of a WEA Alert Message for LTE beyond the current FCC 90 displayable character rule.

Table 5: Considerations for WEA Alert Message Length Option 1

Maximum Length			• GSM/UMTS: 93 per page • LTE: approximately 280 displayable characters subject to technology confirmation by ATIS standards • CDMA 4800bps: Variable, but 90 guaranteed • CDMA 9600bps: Variable, but 90 guaranteed
Existing WEA Elements & Interfaces	**EOC**	**Alert Originator**	In order to accommodate existing base of 2G/3G and LTE WEA-enabled mobile devices, as well as future LTE mobile devices capable of receiving longer messages, the Alert Originator would need to create two WEA Alert Messages, the first adhering to the 90 displayable character maximum and the second to support the longer displayable character length. Alternatively, a longer displayable character message may be created where the first 90 displayable characters remain per the current FCC rules and are delivered to legacy devices, and the full longer displayable characters are delivered to future enhanced WEA LTE mobile devices.
		Alert Origination Tool	Alert Origination Tool would need to create both the 90 displayable character WEA Alert Message and the longer displayable character WEA Alert Message in order to support both legacy mobile devices and future enhanced WEA capable LTE mobile devices. Alert Origination Tool would need to support two versions (with different lengths) of the WEA Alert Message in the CAP message.
	FEMA IPAWS	**Aggregator**	If verification includes checking adherence to 90 displayable characters, then it would need to be modified accordingly. Modifications to the FEMA IPAWS would be required to support both the 90 displayable character and the longer displayable character message from the Alert Originator.
		Gateway	If verification includes checking adherence to 90 displayable characters, then it would need to be modified accordingly. Modifications to the FEMA IPAWS would be required to support both the 90 displayable character and the longer displayable character message.
	CMSP	**Gateway**	If verification includes checking adherence to 90 displayable characters, then it would need to be modified accordingly. Modifications to the CMSP WEA infrastructure would be required to send the 90 displayable character WEA Alert Message to 2G/3G networks and the future longer displayable character WEA Alert Message to LTE networks.

			Modifications would be required to Joint ATIS/TIA CMAS standards for C-Interface and C-Interface testing.
		Core Network and Radio Elements	Modifications to the CMSP infrastructure would be required to support the future longer displayable character WEA Alert Message in LTE networks. Modifications would be required to the 3GPP standards to also support the longer WEA Alert Messages for LTE and to support inbound international roamers.
		Mobile Device	New mobile devices would be required to support the longer displayable character WEA Alert Message (as well as legacy support). Modifications would be required to the 3GPP standards to also support the longer displayable character WEA Alert Messages for LTE and to support inbound international roamers. Modifications would be required to Joint ATIS/TIA CMAS standards for mobile device behavior.
	Interfaces	**A**	CAP message would need to support both the 90 displayable character WEA Alert Message and the longer displayable character WEA Alert Message.
		B	CAP message would need to support both the 90 displayable character WEA Alert Message and the displayable character WEA Alert Message.
		C	Modifications to the C interface would be required to support the legacy 90 displayable character message and the longer displayable character WEA Alert Message.
		D	Modifications to the CMSP WEA infrastructure would be required.
		E	Modifications to the CMSP infrastructure would be required. Modifications would be required to the 3GPP standards to also support the longer WEA Alert Messages and to support inbound international roamers.
Non-WEA Elements	**CMSP**	**WiFi**	Not Applicable.
		Data Session	Not Applicable.
Implications for Mobile Device app Enhancements			Not Applicable.
Trusted Server			Not Applicable.
Pros			Leverages built-in capabilities in LTE networks. Retransmission capabilities handle missed messages. This method leverages and is backwards compatible with existing WEA implementations. Supports Participating CMS provider obligations under the WARN Act.
Cons			Potential user confusion about both 90 displayable character and longer displayable character messages.

	Alert Originators would need to create 90 displayable character and longer displayable character messages.
Challenges with Regard to WARN Act	None.
Mitigating Factors	LTE is the common denominator for enhanced WEA so no changes to CDMA, GSM, or UMTS would be required. Consumer outreach on two different WEA Alert Message sizes. FEMA training for Alert Originators and updates to Alert Originator tools.

C.2. WEA Alert Message Length Option 2 – Packet-Based Concatenation

GSM/UMTS standards support the concatenation up to fifteen pages resulting in a maximum of 1,381 characters. The LTE standards have the theoretical ability to concatenate 32 pages resulting in a maximum of about 10,000 characters. CDMA Cell Broadcast standards do not support concatenation. This concatenation option poses significant network engineering and operational challenges; thus making this option impractical.

In order to maintain consistency across all 2G/3G technologies, the existing 90 displayable character length should be maintained for the legacy technologies. LTE supports longer message lengths per page.

Table 6: Considerations for WEA Alert Message Length Option 2

Maximum Length			GSM/UMTS: 1,381 LTE: 10,081 (theoretical limit; not a practical limit) CDMA: NA (concatenation not supported)
Existing WEA Elements & Interfaces	**EOC**	**Alert Originator**	In order to accommodate existing base of 2G/3G and LTE WEA-enabled mobile devices, as well as future LTE mobile devices capable of receiving longer messages, the Alert Originator would need to create two WEA Alert Messages, the first adhering to the 90 displayable character maximum and the second to the longer displayable character maximum. Alternatively, a longer displayable character message may be created where the first 90 displayable characters remain per the current FCC rules and are delivered to legacy devices, and the full longer displayable characters are delivered to future enhanced WEA LTE mobile devices.
		Alert Origination Tool	Alert Origination Tool would need to create both the 90 displayable character WEA Alert Message and the longer WEA Alert Message in order to support both legacy 2G/3G mobile devices and future enhanced WEA capable LTE mobile devices. Alert Origination Tool would need to support two versions (with different lengths) of the WEA Alert Message in the CAP message.
	FEMA IPAWS	**Aggregator**	If verification includes checking adherence to 90 displayable characters, then it would need to be modified accordingly. Modifications to the FEMA IPAWS would be required to support both the 90 displayable character and the longer displayable character message from the Alert Originator.
		Gateway	If verification includes checking adherence to 90 displayable characters, then it would need to be modified accordingly. Modifications to the FEMA IPAWS would be required to support both the 90 displayable character and the longer displayable character message.
	CMSP	**Gateway**	If verification includes checking adherence to 90 displayable characters, then it would need to be modified accordingly. Modifications to the CMSP WEA infrastructure would be required.

			Modifications would be required to Joint ATIS/TIA CMAS standards for C-Interface and C-Interface testing.
		Core Network and Radio Elements	Modifications to the CMSP infrastructure would be required. Modifications would be required to the 3GPP standards to also support the longer displayable character WEA Alert Messages and to support inbound international roamers.
		Mobile Device	New mobile devices would be required to support the longer displayable character WEA Alert Message (as well as legacy support). Modifications would be required to the 3GPP standards to also support the longer displayable character WEA Alert Messages for LTE and to support inbound international roamers. Modifications would be required to Joint ATIS/TIA CMAS standards for mobile device behavior.
	Interfaces	**A**	CAP message would need to support both the 90 displayable character WEA Alert Message and the longer displayable character WEA Alert Message.
		B	CAP message would need to support both the 90 displayable character WEA Alert Message and the longer displayable character WEA Alert Message.
		C	Modifications to the C interface would be required to support the legacy 90 displayable character message and the longer displayable character WEA Alert Message.
		D	Modifications to the CMSP WEA infrastructure would be required.
		E	Modifications to the CMSP infrastructure would be required. Modifications would be required to the 3GPP standards to also support the longer displayable character WEA Alert Messages and to support inbound international roamers.
Non-WEA Elements	**CMSP**	**WiFi**	Not Applicable.
		Data Session	Not Applicable.
Implications for Mobile Device app Enhancements			Not Applicable.
Trusted Server			Not Applicable.
Pros			Leverages built-in capabilities in GSM/UMTS/LTE cellular networks. This includes retransmission capabilities to handle dropped/lost packets. This method leverages and is backwards compatible with existing WEA implementation. Supports Participating CMS provider obligations under the WARN Act.
Cons			Not applicable to CDMA-based cellular systems. Is not required for supporting the longer displayable character messages in LTE.

	Depending on message length, dropped/lost pages would induce variable delays in the presentation of the WEA Alert Message to the mobile device user. Not all legacy GSM/UMTS mobile devices support multiple page Cell Broadcast messages. As consequence, if this were considered for legacy GSM/UMTS, two WEA Alert Messages may need to be broadcast. One message being the legacy 90 displayable character WEA Alert Message and the other message being the longer enhanced WEA Alert Message. Even though more than longer displayable characters WEA Alert Messages can be broadcast, the form factors of various types and models of mobile devices to not easily facilitate the presentation of very large alert messages.
Challenges with Regard to WARN Act	None.
Mitigating Factors	None.

C.3. WEA Alert Message Length Option 3 – Message-Based Concatenation

The wireless carrier transmits the original alert message as a sequence of complete WEA Alert Messages. The WEA OS app is programmed to retrieve that sequence from the WEA inbox, concatenate them, and then present to the end-user.

Table 7: Considerations for WEA Alert Message Length Option 3

Maximum Length			Limited by the length of time required for the mobile device to receive and concatenate the components of the longer WEA Alert Message. Unknown until completion of feasibility study.
Existing WEA Elements & Interfaces	**EOC**	**Alert Originator**	In order to accommodate existing base of 2G/3G and LTE WEA-enabled mobile devices, as well as future mobile devices capable of receiving these longer concatenated messages, the Alert Originator would need to create two WEA Alert Messages, the first adhering to the 90 displayable character maximum and the second to the longer WEA Alert Message.
		Alert Origination Tool	Alert Origination Tool would need to create both the 90 displayable character WEA Alert Message and the longer displayable WEA Alert Message in order to support both legacy mobile devices and future enhanced WEA capable mobile devices. Alert Origination Tool would need to support two versions of the WEA Alert Message in the CAP message. Mechanism must be defined on how the sequencing of messages is performed and identified within the message.
	FEMA IPAWS	**Aggregator**	Would need to accommodate CAP messages with at least two versions of the WEA Alert Message. The first is for 90 displayable character WEA Alert Message, and the second is for the sequence of 90 displayable character WEA Alert Messages. Modifications to the FEMA IPAWS would be required to support both the 90 displayable character and sequence of 90 displayable character WEA Alert Messages from the Alert Originator.
		Gateway	Would need to accommodate CAP messages with at least two versions of the WEA Alert Message. The first is for 90 displayable character WEA Alert Message, and the second is for the sequence of 90 displayable character WEA Alert Messages. Modifications to the FEMA IPAWS would be required to support both the 90 displayable character and the sequence of 90 displayable character WEA Alert Messages.
	CMSP	**Gateway**	Modifications to the CMSP WEA infrastructure would be required. Modifications would be required to Joint ATIS/TIA CMAS standards and C-Interface and C-Interface testing. Backward compatibility with existing WEA implementations as well as future implementation options would need to be addressed in the feasibility study.

		Core Network and Radio Elements	Modifications to the CMSP infrastructure may be required. Modifications may be required to the 3GPP standards to support the sequencing of the multi-part WEA Alert Messages and to support inbound international roamers. Backward compatibility with existing WEA implementations as well as future implementation options would need to be addressed in the feasibility study.
		Mobile Device	A feasibility study would need to be performed to determine if a potential mechanism exists to support this alternative. If such a mechanism exists, that mechanism would need to be standardized and developed for the mobile device to correlate the received messages and to assemble the individual WEA Alert Messages into a longer single alert message. New mobile devices would be required to support both the 90 displayable character WEA Alert Message and the longer multi-part WEA Alert Message. Modifications may be required to the 3GPP standards to also support the multi-part WEA Alert Messages and to support inbound international roamers. Modifications would be required to Joint ATIS/TIA CMAS standards for mobile device behavior. Backward compatibility with existing WEA implementations as well as future implementation options would need to be addressed in the feasibility study.
	Interfaces	**A**	CAP message would need to support both the 90 displayable character WEA Alert Message and the sequence of 90 displayable character WEA Alert Messages.
		B	CAP message would need to support both the 90 displayable character WEA Alert Message and the sequence of 90 displayable character WEA Alert Messages.
		C	Modifications to the C interface would be required to support the legacy 90 displayable character message and the sequence of 90 displayable character WEA Alert Messages.
		D	Modifications to the CMSP WEA infrastructure would be required.
		E	Modifications to the CMSP infrastructure would be required. Modifications would be required to the 3GPP standards to also support the longer multi-part WEA Alert Messages and to support inbound international roamers.
Non-WEA Elements	**CMSP**	**WiFi**	Not Applicable.
		Data Session	Not Applicable.
Implications for Mobile Device app Enhancements			Not Applicable.
Trusted Server			Not Applicable.
Pros			Has the potential to support longer length for WEA Alert Messages.

Cons	There is no mechanism in existing standards to perform this sequencing of the longer WEA Alert Message into individual 90 displayable character messages. This alternative would require a feasibility study and, if feasible, followed by a standardization effort as well as development. This method is not backwards compatible with existing WEA standards and implementations. The mobile device may not receive every individual WEA Alert Message of the sequence of WEA Alert Messages due to transmission errors, coverage gaps, edge of coverage boundary, etc. The mobile device may have difficulty determining the individual WEA Alert Messages of the sequence and not conflict with the duplicate message detection functionality. This method may be problematic at boundaries of technologies (e.g., UMTS and LTE) when a mobile moves between technologies and receives only some of the multi-part message before the transition. Modifications would be required to the 3GPP standards to support the longer WEA Alert Messages, the sequencing and to support inbound international roamers; because the underlying standards/technology already supports longer message lengths it is unlikely that this methodology would be seriously considered in any regional or global standards. Multi-part messages increase network traffic load. Broadcast of all message parts may be delayed depending upon traffic and congestion conditions. Retransmission frequency is based upon the wireless operator network traffic load, the number of WEA Alert Messages, and the number parts for a WEA Alert Message. There may a significant amount of time between the retransmission of an individual part of a multi-part WEA Alert Message. Presentation of reconstructed alert message to the subscriber may be delayed if one or more components of the message are not received error-free and a wait for rebroadcast of one or more messages is required. Dropped/lost messages would delay presentation of the WEA Alert Message to the mobile device user. Even though longer displayable characters can be broadcast, the form factors of various types and models of mobile devices to not easily facilitate the presentation of very large alert messages. Requires software changes to the mobile device or new mobile devices.
Challenges with Regard to WARN Act	None.
Mitigating Factors	None.

C.4. WEA Alert Message Length Option 4 – Human-Based Concatenation

The original alert message is partitioned into multiple smaller (90 displayable character maximum) alert messages before delivery to the CMSP, adding page numbers to each of the smaller alert messages [e.g., (1/3), (2/3), (3/3)]. Therefore, the original alert message is delivered to the CMSP as multiple individual WEA Alert Messages, and the end-user is relied upon to read them in the correct order.

A feasibility study would need to be performed to determine a practical mechanism for the partitioning and management of the WEA Alert Message.

Table 8: Considerations for WEA Alert Message Length Option 4

Maximum Length			Limited by the length of time required for the mobile device to receive the components of the longer WEA Alert Message.
Existing WEA Elements & Interfaces	**EOC**	**Alert Originator**	None as it assumed that all WEA Alert Messages can be concatenated by the human mobile device user.
		Alert Origination Tool	Pending the results of the feasibility study, if participating is performed at the Alert Origination Tool, then the Alert Origination Tool would need modifications to generate multiple 90 displayable character messages which include the appropriate (n/m) sequencing. The Alert Origination Tool must also manage alert updates and alert cancellations for all messages in the sequence.
	FEMA IPAWS	**Aggregator**	Assuming the Alert Origination Tool breaks the longer message into smaller parts, ideally each part of the message in the sequence would have to be sent to the Aggregator at approximately the same time so that each message is delivered to the CMSP Gateway at approximately the same time. May need to accommodate CAP messages to support delivery all segments of the message in one CAP message.
		Gateway	As above, each part of the message in the sequence would have to be sent to the Gateway at the same time so that each message ultimately is transmitted at the same time. May need to accommodate CAP messages to support delivery all segments of the message in one CAP message. The Federal Alert Gateway then sends each 90 displayable character part of the message to the CMSP Gateway as individual C interface messages.
	CMSP	**Gateway**	If there is no sequencing or correlation of the individual messages in the CMS provider infrastructure, then there is no impact.
		Core Network and Radio Elements	If there is no sequencing or correlation of the individual messages in the CMS provider infrastructure, then there is no impact.
		Mobile Device	There will be user interaction problems in many devices. The user interface may not allow the user to effectively concatenate the multiple alert messages.
	Interfaces	**A**	CAP message would need to support both the 90 displayable

			character WEA Alert Message and the longer multi-part WEA Alert Messages.
		B	CAP message would need to support both the 90 displayable character WEA Alert Message and the longer multi-part WEA Alert Messages.
		C	Modifications to the C interface would be required to support the legacy 90 displayable character message and the longer multi-part WEA Alert Messages.
		D	None.
		E	None.
Non-WEA Elements	**CMSP**	**WiFi**	Not Applicable.
		Data Session	Not Applicable.
Implications for Mobile Device app Enhancements			Not Applicable.
Trusted Server			Not Applicable.
Pros			Supports longer length for WEA Alert Messages.
Cons			Presents numerous human factors challenges. May be strenuous for humans to do manual eye-balling-based concatenation. Individuals with disability especially cognitive disabilities will find this method difficult and confusing. Assumes a particular implementation in the mobile device. At least one smartphone OS does not store the WEA Alert Messages. Many smartphone implementations only display one alert message at a time. Therefore, the subscriber would have to read each message individually and remember the message content. Subscriber may not receive the multiple WEA Alert Messages in numerical order. For example, the first message received by mobile device may be 2 of 3. If several multi-part alert messages are being broadcast at the same time, the subscriber will have difficulty identifying which parts of which message belong together and thus will have difficulty understanding the alert messages. For example, does the 2 of 3 message received apply to the Flash Flood alert message or the Severe Thunderstorm alert message? Mobile device may not receive every page of WEA Alert Message due to transmission errors, coverage gaps, edge of coverage boundary, etc. Multi-part messages increase network traffic load. Broadcast of all message parts may be delayed depending upon traffic and congestion conditions. Retransmission frequency is based upon the wireless operator network traffic load, the number of WEA Alert Messages, and the number parts for a WEA Alert Message. There may

	a significant amount of time between the retransmission of an individual part of a multi-part WEA Alert Message.
Challenges with Regard to WARN Act	None.
Mitigating Factors	None.

C.5. WEA Alert Message Length Option 5 – Fewer Bits per Character

Today, the CMSP infrastructure including the radio elements uses an internationally standardized and recognized 7-bits-per-character encoding scheme (3GPP TS 23.038), resulting in a maximum of 630 bits in a 90 displayable character FCC defined WEA Alert Message. It is possible, if defined in global standards, to use alternate character sets that use fewer bits per character. By reducing the number of bits per character, this option can increase the number of characters accommodated by 630 bits.

Methods to reduce the number of bits per character require further research as well as further study and standardization in ATIS and/or 3GPP. Methods to reduce the number of bits per character may include new encoding schemes, e.g., at the application layer. Typical methods to reduce the number of bits per character are (a) eliminating unused characters from the allowable character set, and (b) exploiting statistical characteristics of WEA Alert Messages.

Table 9: Considerations for WEA Alert Message Length Option 5

Maximum Length			Further study would be needed to determine the maximum displayable character length. However, for 2G and 3G networks, 140 displayable characters seems within reach, but research, standardization, lab testing, and evaluation would be needed to investigate the limit more thoroughly and to describe a bit representation scheme for reaching that limit. Further study would be needed to identify the maximum displayable character message in LTE.
Existing WEA Elements & Interfaces	**EOC**	**Alert Originator**	In order to accommodate existing base of 2G/3G and LTE WEA-enabled mobile devices, as well as future mobile devices capable of using a method as described here, the Alert Originator would need to create at least two WEA Alert Messages, the first adhering to the 90 displayable character maximum and the second to the maximum that this method would support (140 characters).
		Alert Origination Tool	Alert Origination Tool would need to create both the 90 displayable character WEA Alert Message and the encoded longer WEA Alert Message in order to support both legacy mobile devices and future enhanced mobile devices using this method. Alert origination tools with the 90 displayable character limit built into them would need to adjust that limitation. Alert Origination Tool would need to support multiple versions (with different lengths and different character formatting) of the WEA Alert Message in the CAP message. Alert Origination Tool would need to re-encode message using more efficient bit representation and needs to indicate in the CAP message that this is the new format encoded WEA Alert Message.
	FEMA IPAWS	**Aggregator**	Would need to accommodate CAP messages with multiple versions of the WEA Alert Message. Modifications to the FEMA IPAWS would be required to support the multiple formats of the WEA Alert Message from the Alert Originator.

		Gateway	Would need to accommodate CAP messages with multiple versions of the WEA Alert Message. Modifications to the FEMA IPAWS would be required.
	CMSP	**Gateway**	Would need to accommodate C interface messages with multiple versions of the WEA Alert Message. Modifications to the CMSP WEA infrastructure would be required. Modifications would be required to Joint ATIS/TIA CMAS standards including the C-Interface and C-Interface testing and related 3GPP specifications.
		Core Network and Radio Elements	Modifications to the CMSP infrastructure would be required. At a minimum, different message identifiers have to be used for the various message varieties. Modifications would be required to the 3GPP standards to support the longer WEA Alert Messages with the different character encoding and to support inbound international roamers.
		Mobile Device	Modifications to mobile devices would be required to support both the 90 displayable character WEA Alert Message and the enhanced WEA Alert Message with the different character encoding. Modifications would be required to the 3GPP standards to also support the longer WEA Alert Messages with the different character encoding and to support inbound international roamers. Modifications would be required to Joint ATIS/TIA CMAS standards for mobile device behavior.
	Interfaces	**A**	CAP message would need to support both the 90 displayable character WEA Alert Message and the enhanced longer WEA Alert Message with different character encoding, and a longer WEA Alert Message for LTE.
		B	CAP message would need to support both the 90 displayable character WEA Alert Message and the enhanced longer WEA Alert Message with different character encoding, and a longer WEA Alert Message for LTE.
		C	Modifications to the C interface would be required to support the legacy 90 displayable character message, the enhanced longer WEA Alert Message with different character encoding, and the longer WEA Alert Message for LTE.
		D	Modifications to the CMSP WEA infrastructure would be required. At a minimum, different message identifiers have to be used for the various message varieties.
		E	Modifications to the CMSP infrastructure would be required. At a minimum, different message identifiers have to be used for the various message varieties. Modifications would be required to the 3GPP standards to also support the enhanced WEA Alert Messages with the different character encoding and to support inbound international roamers.
Non	**CMSP**	**WiFi**	Not Applicable.

		Data Session	Not Applicable.
Implications for Mobile Device app Enhancements			Not Applicable.
Trusted Server			Not Applicable.
Pros			Further study would be needed, however a 140-character limit for 2G and 3G may be within reach. Further research would be needed to determine the maximum potential character length for LTE.
Cons			Further research and standards activity would be needed as it is not clear how many characters this method may support. Alternate character sets and compression technique are not required for GSM/UMTS based or LTE based WEA Alert Messages since these technologies can already support more than 90 displayable character WEA Alert Messages. The 7 bit GSM character set is globally recognized and implemented. Adding new character sets would pose challenges including backward compatibility and support of international roamers. There are backward compatibility issues as well as concerns that a device that does not understand the encoding will be presenting gibberish to the user. Modifications would be required to the 3GPP standards to support new character sets and to support inbound international roamers.
Challenges with Regard to WARN Act			None.
Mitigating Factors			None.

C.6. WEA Alert Message Length Option 6 – Downloading Over Cellular Connection

Upon receiving the existing 90 displayable character WEA Alert Message, the mobile device can be programmed to treat the cell broadcast reception of a WEA Alert Message as a trigger to fetch more detailed information from a trusted source using the mobile device's cellular data connection. The "fetch" could be automatic, or it could be a "clickable" or "non-clickable" URL embedded in the 90 displayable character WEA Alert Message that the user would select if more detailed information is desired.

The "detailed information" from the trusted source should be limited in size, for example it may be a longer text message (e.g., 280-characters). This "retrieval from trusted source" is outside the scope of carrier obligations under WEA (both FCC rules and the WARN Act).

The "detailed information" is generated by the Alert Originator, is sent to FEMA IPAWS where the detail information is then sent to the "trusted source" to be available for mobile devices to retrieve.

The trusted source must have a well-known address that is either pre-provisioned in the mobile device and not included as part of the WEA Alert Message, or optionally included in the 90 displayable character WEA broadcast.

Table 10: Considerations for WEA Alert Message Length Option 6

Maximum Length			Would have to be determined via a standardization process between the wireless operators, DHS S&T, FEMA and the Alert Originator community.
Existing WEA Elements & Interfaces	**EOC**	**Alert Originator**	The Alert Originator may need to create two WEA Alert Messages, the first adhering to the 90 displayable character maximum and the second the detailed information for the trusted source. The Alert Originator would need the capability to create the more detailed information, e.g., longer message, for the trusted source.
		Alert Origination Tool	The Alert Originator Tool would need the capability to create both a 90 displayable character WEA Alert Message and the more detailed information for the trusted source.
	FEMA IPAWS	**Aggregator**	FEMA IPAWS would need modifications to receive from the Alert Originator the 90 displayable character WEA Alert Message and to support and/or deliver the more detailed information to the trusted source whenever a WEA Alert Message is sent to the wireless operators. Modifications to the FEMA IPAWS would be required to support receiving the information from the Alert Originator to be sent to the trusted source.
		Gateway	FEMA IPAWS would need modifications to receive from the Alert Originator the 90 displayable character WEA Alert Message and to support and/or deliver the more detailed information to the trusted source whenever a WEA Alert Message is sent to the wireless operators.

	CMSP	**Gateway**	None unless a different cell broadcast message identifier is used. If a different message ID is used, modifications would be required to the 3GPP standards support the message ID and to support inbound international roamers. If a different message ID is used, modifications to the CMSP WEA infrastructure would be required. If a different message ID is used, modifications would be required to Joint ATIS/TIA CMAS standards for C-Interface and C-Interface testing.
		Core Network and Radio Elements	None – this assumes a standard 90 displayable character WEA Alert Message will be used. If a different cell broadcast message ID is used to differentiate this capability, modifications would be required to the 3GPP standards to also support the new message id and to support inbound international roamers.
		Mobile Device	New mobile devices would be required to support the ability to retrieve the more detailed information when a WEA Alert Message is received, or alternatively developing APIs which expose the WEA Alert Message to apps on the mobile device so an app could be developed to retrieve more detailed information. This option could be supported natively in the mobile device without a third-party app. Modifications would be required to Joint ATIS/TIA CMAS standards for mobile device behavior.
	Interfaces	**A**	CAP message would need to support both the 90 displayable character WEA Alert Message and the longer WEA Alert Message with indication of the trusted source.
		B	CAP message would need to support both the 90 displayable character WEA Alert Message and the longer WEA Alert Message with indication of the trusted source.
		C	If a different message ID is used, modifications would be required to Joint ATIS/TIA CMAS standards for C-Interface and for C-Interface testing.
		D	If a different message ID is used, modifications to the CMSP WEA infrastructure would be required.
		E	If a different message ID is used, modifications would be required to the 3GPP standards to also support the longer WEA Alert Messages and to support inbound international roamers.
Non-WEA Elements	**CMSP**	**WiFi**	Not Applicable.
		Data Session	A separate data session would have to be established via the cellular connection. This option requires the subscriber to have a data plan and these sessions will be charged to the subscriber's data plan. Alternatively, this could be a subscription based service paid for by the trusted source.
Implications for Mobile Device app			One implementation option is to have a mobile device app with

Enhancements	the intelligence to execute method as described. Alternatively, this could be a component of the WEA functionality on the mobile device. Would need significant changes to mobile device functionality to support this alternative and any mobile device app implementation options.
Trusted Server	One implementation option is to provide information to mobile device app upon request in a secure, reliable and scalable fashion. May also need to be connected to FEMA IPAWS; security may be problematic for untrusted mobile devices connecting to FEMA IPAWS directly.
Pros	Supports longer length for WEA Alert Messages.
Cons	Use of the cellular network for additional data may be disruptive by overloading the network and may adversely impacting voice and data services including 9-1-1 emergency calls and Wireless Priority Service (WPS). 'Automatic" retrieval of data may be worse than allowing users to retrieve on their own. This alternative is susceptible to congestion on CMSP networks, and depending on how many WEA devices are attempting to retrieve detailed information from a given cell site or group of cell sites, the results could be anywhere from reduced throughput for each user (slowing the retrieval of the detailed information) to congestion/blockage of voice and data traffic in the cell(s). The trusted source could also experience congestion, especially if there are a significant number of alerts throughout the country at the same time (e.g., similar effect to the recent Twitter congestion from the number of retweets of the photo from the Grammy's). The trusted server may be overloaded. The alternative must scale for potential nationwide alerts covering 300+ million mobile devices. May exclude providing alert information to classes of users that either do not use cellular data or cannot afford smartphones or data services. There are no mobile device APIs defined for third party apps to receive the information. Standards would have to be developed. There is no information in the WEA text message to correlate it to the original alert message. There is no room in the existing 90 displayable character message to add an indication of the original alert message. The WEA Alert Message text is not unique enough to correlate to the original message. If the indication to the original message is included in the 90 displayable characters, legacy mobile devices will display this indication which is appear as gibberish to the mobile device user. Use of a different message ID to provide the information on the location of the information on the trusted server would need development efforts for the CMSP infrastructure. Support of a different message ID to provide the information

	on the location of the information on the trusted server also requires mobile device modifications. This option assumes a particular implementation in the mobile device. At least one smartphone OS does not store the WEA Alert Messages in a WEA inbox. Therefore, it will not be possible for a WEA app to retrieve that alert message on that smartphone OS. An entity has to be identified and established to be the "trusted source". The trusted source would need to open their systems to every mobile device in the world with no security mechanisms. It can be envisioned that malware or man-in-the-middle attacks could be used to cause havoc. Even though a larger number of displayable characters can be obtained, the form factors of various types and models of mobile devices to not easily facilitate the presentation of very large alert messages. This alternative requires the subscriber to have a data plan and these sessions will be charged to the subscriber's data plan. Alternatively, this could be a subscription based service paid for by the trusted source.
Challenges with Regard to WARN Act	This alternative does not meet the WARN Act requirements. The Participating CMS provider is not responsible for the trusted source or retrieval process. This alternative is beyond the obligations of the CMSPs and outside of the scope of the WARN Act. WARN specifically states that WEA alerts are to be provided at no cost to the subscribers. However, retrieval of additional information from the trusted source would incur charges to the subscriber's data plan.
Mitigating Factors	Some users may do this on their own today to seek additional information. There may be potentially many sources of information to which they can turn. There are techniques available to handle potential overloading of trusted servers. Content staging and load balancing are examples of potential mitigations for the overloading of trusted server. To correlate the message at the trusted server with the WEA alert, additional information must be provided in the WEA Alert Message. Additional study would be required to evaluate the character limitations and capabilities available in LTE. Network integrity standards could be developed that would limit use of this alternative to messages that would not trigger reactions close to network capability limitations. Use this alternative only for localized emergency events and not for large scale WEA alerts or nationwide Presidential alerts to reduce impact to the trusted server. The ATIS/TIA standards body would need to evaluate this alternative and provide any mitigating factors to the impacts to the cellular networks. The FCC would need to work with Congress on exemption on

	subscriber charges for retrieval of the additional information from the trusted source. If an exemption is not available, mechanisms for handling would be required. ATIS/TIA would need to perform a feasibility study of not charging the subscribers for the data retrieval from the trusted source and charging the trusted source for any associated data retrievals of the additional information.

C.7. WEA Alert Message Length Option 7 – Downloading Over WiFi Connection

Upon receiving the existing 90 displayable character WEA Alert Message, the mobile device can be programmed to treat the cell broadcast reception of a WEA Alert Message as a trigger to fetch more detailed information from a trusted source using the mobile device's WiFi connection (if available). The "fetch" could be automatic, or it could be a "clickable" or "non-clickable" URL embedded in the 90 displayable character WEA Alert Message that the user would select if more detailed information is desired.

The "detailed information" from the trusted source should be limited in size, for example it may be a longer text message (e.g., 280-characters). This "retrieval from trusted source" is outside the scope of carrier obligations under WEA (both FCC rules and the WARN Act).

The "detailed information" is generated by the Alert Originator, is sent to FEMA IPAWS where it is then sent to the "trusted source" to be available for mobile devices to retrieve.

The trusted source must have a well-known address that is either pre-provisioned in the mobile device and not included as part of the WEA Alert Message, or optionally included in the 90 displayable character WEA broadcast.

Table 11: Considerations for WEA Alert Message Length Option 7

Maximum Length			Would have to be determined via a standardization process between the wireless operators, DHS S&T, FEMA and the Alert Originator community.
Existing WEA Elements & Interfaces	**EOC**	**Alert Originator**	The Alert Originator may need to create two WEA Alert Messages, the first adhering to the 90 displayable character maximum and the second the detailed information for the trusted source. The Alert Originator would need the capability to create the more detailed information, e.g., longer message, for the trusted source.
		Alert Origination Tool	The Alert Originator Tool would need the capability to create both a 90 displayable character WEA Alert Message and the more detailed information for the trusted source.
	FEMA IPAWS	**Aggregator**	FEMA IPAWS would need modifications to receive from the Alert Originator the 90 displayable character WEA Alert Message and to support and/or deliver the more detailed information to the trusted source whenever a WEA Alert Message is sent to the wireless operators. Modifications to the FEMA IPAWS would be required to support receiving the information from the Alert Originator to be sent to the trusted source.
		Gateway	FEMA IPAWS would need modifications to receive from the Alert Originator the 90 displayable character WEA Alert Message and to support and/or deliver the more detailed information to the trusted source whenever a WEA Alert Message is sent to the wireless operators.
	CMSP	**Gateway**	None unless a different cell broadcast message identifier is

			used. If a different message ID is used, modifications would be required to the 3GPP standards support the message ID and to support inbound international roamers. If a different message ID is used, modifications to the CMSP WEA infrastructure would be required. If a different message ID is used, modifications would be required to Joint ATIS/TIA CMAS standards for C-Interface and C-Interface testing.
		Core Network and Radio Elements	None – this assumes a standard 90 displayable character WEA Alert Message will be used. If a different cell broadcast message ID is used to differentiate this capability, modifications would be required to the 3GPP standards to also support the new message id and to support inbound international roamers.
		Mobile Device	New mobile devices would be required to support the ability to retrieve the more detailed information when a WEA Alert Message is received. This detailed information retrieval would be from a WiFi connection when the WiFi connection is available on the mobile device. Modifications would be required to Joint ATIS/TIA CMAS standards for mobile device behavior.
	Interfaces	**A**	CAP message would need to support both the 90 displayable character WEA Alert Message and the longer WEA Alert Message with indication of the trusted source.
		B	CAP message would need to support both the 90 displayable character WEA Alert Message and the longer WEA Alert Message with indication of the trusted source.
		C	If a different message ID is used, modifications would be required to Joint ATIS/TIA CMAS standards for C-Interface and C-Interface testing.
		D	If a different message ID is used, modifications to the CMSP WEA infrastructure would be required.
		E	If a different message ID is used, modifications would be required to the 3GPP standards to also support the longer WEA Alert Messages and to support inbound international roamers.
Non-WEA Elements	**CMSP**	**WiFi**	The mobile device would need to check to see if a WiFi connection is active to allow retrieval from the trusted source.
		Data Session	None.
Implications for Mobile Device app Enhancements			One implementation option is to have a mobile app with the intelligence to execute method as described. Would need significant changes to mobile device functionality to support this alternative and any mobile device app implementation options.
Trusted Server			One implementation option is provide information to mobile device app upon request in a secure, reliable and scalable fashion.

	May also need to be connected to FEMA IPAWS; security may be problematic for untrusted mobile devices connecting to FEMA IPAWS directly.
Pros	Supports longer WEA Alert Messages for a subset of mobile devices which have an active WiFi connection. Use of WiFi offloads traffic from the cellular network.
Cons	It cannot be assumed that mobile devices are connected to WiFi. • Mobile devices may not automatically connect to WiFi without some other type of user intervention. • Not every mobile device may have WiFi capabilities. • Subscriber may have turned off the WiFi connection. • Subscriber may not have configured WiFi connections. • WiFi connections generally not available in rural and remote locations. • WiFi connections may not be available in suburban locations beyond subscriber's home or neighborhood stores (e.g., coffee shop). • If driving in a car, the mobile device may be connected to WiFi within the car but the car is not WiFi connected to external access points. • WiFi connections may not be free and the subscriber may not be subscribed to the WiFi service. Network congestion of WiFi connections may occur. The trusted server may be overloaded. The alternative must scale for potential nationwide alerts covering 300+ million mobile devices. Mobile device modifications would be required to limit the data retrieval to only WiFi connections. There are no mobile device APIs defined for third party apps to receive the information. There is no information in the WEA text message to correlate it to the original alert message. There is no room in the existing 90 displayable character message to add an indication of the original alert message. The WEA Alert Message text is not unique enough to correlate to the original message. If the indication to the original message is included in the 90 displayable characters, legacy mobile devices will display this indication which is appear as gibberish to the mobile device user. Use of a different message ID to provide the information on the location of the information on the trusted server would need development efforts for the CMSP infrastructure. Support of a different message ID to provide the information on the location of the information on the trusted server also requires mobile device modifications. This option assumes a particular implementation in the mobile device. At least one smartphone OS does not store the WEA

	Alert Messages in a WEA inbox. Therefore, it will not be possible for a WEA app to retrieve that alert message on that smartphone OS. An entity has to be identification established to be the "trusted source". The trusted source would need to open their systems to every mobile device in the world with no security mechanisms. It can be envisioned that malware or man-in-the-middle attacks could be used to cause havoc. Even though a larger number of displayable characters can be obtained, the form factors of various types and models of mobile devices to not easily facilitate the presentation of very large alert messages.
Challenges with Regard to WARN Act	This alternative does not meet the WARN Act requirements. The Participating CMS provider is not responsible for the trusted source or retrieval process. This alternative is beyond the obligations of the CMSPs and outside of the scope of the WARN Act.
Mitigating Factors	Some users may do this on their own today to seek additional information. There may be potentially many sources of information to which they can turn. There are techniques available to handle potential overloading of trusted servers. Content staging and load balancing are examples of potential mitigations for the overloading of trusted server. To correlate the message at the trusted server with the WEA alert, additional information must be provided in the WEA Alert Message. Additional study would be required to evaluate the character limitations and capabilities available in LTE.

Appendix D: Evaluation of WEA Geo-Targeting Options

This Appendix discusses ideas for enhancing WEA geo-targeting that were suggested by members of the subgroup. Suggestions were accepted from members regardless of their degree of expertise in cellular networks/systems; allowing the inclusion of ideas motivated by expectations that have been shaped by the public's experience with present-day mobility technologies (in particular smartphone-enabled capabilities).

Non-experts in cellular networks/systems may not be aware of certain considerations (e.g., inner workings of cellular networks, cost considerations, international standards considerations, etc.) and limitations. Thus, an analysis which incorporates expertise from wireless industry members follows the description of each idea. The analyses assess the level of practicality given current and foreseeable-future cellular network design and infrastructure. Ideas considered impractical may be revisited as efforts to improve WEA continue over the coming years and standards to support these impractical ideas evolve. Furthermore, the inclusion of ideas, that are subsequently deemed impractical, provides a documented analysis for why some ideas that would otherwise appear obvious to the average person are not implemented in WEA.

Wireless industry members advise that implementation of any idea needs to be vetted and standardized in an accredited global standards organization (e.g., such as 3GPP and its North American Organizational Partner ATIS).

D.1. Enhancements to WEA Geo-Targeting Since Rollout

Since the rollout of WEA, some CMSPs have made several enhancements to WEA geo-targeting that exceed the requirements specified in FCC's First Report and Order including:

1. Allowing the specification of target areas (i.e., geographic areas specified by Alert Originators to receive the alert) using polygons, as opposed to counties.
2. Selecting alert-broadcasting base-stations based on the overlap of their respective coverage areas with the target area, as opposed to selecting base-stations that are simply located within the target area.
3. Broadcasting the alert to a subset of sectors within a cell, whereby the coverage areas of sectors not transmitted to do not overlap with the target area. This enhancement has only been introduced in LTE networks. As the cellular industry continues its migration to LTE, this enhancement will apply to an increasing percentage of mobile devices.

D.2. About Enhancing WEA Geo-Targeting

From the perspective of the Alert Originator, ideal WEA geo-targeting includes:

a) unlimited flexibility and precision in defining the alert area[25];

b) rendering of the WEA alert on all mobile devices within the alert area; and

c) no mobile device outside the alert area rendering the WEA alert.

[25] See Section 3.3 for definition of alert area.

Accordingly from the perspective of the alert originator, enhanced geo-targeting could be achieved through:

1) Increasing the granularity of the alert area as specified/defined by the Alert Originator.
2) Increasing the number of mobile devices within the alert area that render the WEA alert.
3) Decreasing the number of mobile devices outside the alert area that render the WEA alert.

It is important to note that in the context of WEA broadcasting, there is typically a trade-off between 2) and 3) above.

Indeed from the perspective of a CMSP broadcasting WEA alerts, the objective is to attempt to best approximate the alert area with the CMSP broadcast area as close as possible in order to optimize the number of mobile devices within the alert area that present the WEA alert.

The ideas presented in this Appendix can be divided into four categories:

1. Device-oriented ideas.
2. Enablers for device-oriented ideas. This category includes ideas that do not directly enhance geo-targeting, but could enable and/or simplify the implementation of a device-oriented idea.
3. Network-oriented ideas.
4. Ideas involving assistance from a third-party (i.e., a party other than the mobile device and the cellular network).

D.3. About Device's Estimation of Own Location

Several ideas later in this section are based on the device having an estimate of its geographic location (henceforth geo-location estimate). There is a popular notion that the modern mobile device has an accurate geo-location estimate at all times– especially in light of numerous smartphone applications which show the user their location or use the user's geo-location information in some other way. This notion is not 100% correct. Location determination for mobile devices relies on several techniques to achieve that goal including GPS, OTDOA, WiFi SSID cross-referencing, and inertial sensors.[26]

The speed with which the mobile device can obtain an updated geo-location estimate varies from case to case. In addition, the impact to the network as the mobile device obtains its geo-location estimate varies from case to case.

Focusing on GPS in particular, the mobile device does not always acquire the GPS-based estimate of its location via a standalone/autonomous GPS (S-GPS) operation that uses radio signals from satellites alone. In many cases mobile devices rely on Assisted GPS (A-

[26] See http://blog.jammer-store.com/2012/04/10-ways-for-your-smartphone-to-discover-where-you-are/. WiFi SSID is the ID of the WiFi network. There are databases containing the locations of a large number of WiFi networks. The location of the device can therefore be estimated by looking up the location of a WiFi network that is adjacent to it.

GPS).An explanation can be found in 3GPP TS 23.271, titled "Functional stage 2 description of Location Services (LCS)"[27].) A-GPS additionally uses network resources to locate and use the satellites in poor signal conditions, which may arise due to multipath propagation (e.g., bouncing off buildings) and signal weakening (e.g., signal degradation by having to pass through walls, tree cover, various types of construction, etc.) to speed the calculation of the device location. If first turned on in these conditions, some standalone GPS navigation devices may not be able to fix a position due to the fragmentary signal, and a fix may take as long as 12.5 minutes (the time needed to download the GPS almanac and ephemeris and to search the sky for GPS signal). This condition is commonly referred to as a "Cold Start". Under average conditions, S-GPS can provide first position in approximately 30-40 seconds. This condition is commonly referred to as a "Warm Start". If the satellite signals are lost during the acquisition of this information, it is discarded and the standalone system has to perform a Cold Start GPS location from scratch. In A-GPS, the CMSP deploys an A-GPS server. These A-GPS servers download the orbital information from the satellite and store it in a database. An A-GPS-enabled mobile device can connect to these servers and download this information using CMSP network radio bearers such as GSM, CDMA, WCDMA, LTE or even using other wireless radio bearers such as WiFi. Usually the data rate of these bearers is high; hence downloading orbital information takes less time. It is important to note however that A-GPS may use data services of the cellular network.

A-GPS has two primary modes of operation:

1. Mobile Station Based (MSB): The mobile device receives GPS signals from the visible satellites. It also receives GPS data (ephemeris, reference location, reference time) and other optional assistance data from the A-GPS server. (The CMSP continuously logs GPS information from the GPS satellites using an A-GPS server in its system.) Based on the satellite signals and with the help of the above A-GPS data, the mobile device calculates the position.
2. Mobile Station Assisted (MSA): The mobile device receives acquisition assistance, reference time and other optional assistance data from the CMSP. Using that data in conjunction with the GPS signals, the mobile device calculates a 'fix' and relays that 'fix' to a CMSP A-GPS server. Using the data received from the mobile device and the data already present in A-GPS server, the A-GPS server calculates the position of the mobile device and sends the newly calculated position back to the device.

It should be noted that whether a mobile device functions in MSA or MSB mode is determined by how it is designed by its manufacturer, chipset vendor, and CMSP. There is no setting on the device which allows the user or an application to select MSA or MSB mode.

D.4. Device-Oriented Ideas

The ideas presented in this section are based on device-assisted enhancements to geo-targeting. To geo-filter a received alert this, generally, would entail the mobile device using

a) its knowledge of its location (provided it is immediately available to the device and is not "stale"), and

[27] See http://www.3gpp.org/DynaReport/23271.htm.

b) the coordinates of the polygon of the target area.

For example, if a mobile device is outside the target area but receives the alert from a base-station whose broadcast signal traveled beyond the boundary of the polygon, then the mobile device could have a method to determine that it is outside the target alert area, and hence decide not to render the alert. It is important to note that this idea is not new and was fully vetted during the proceedings of CMSAAC, but was challenged with Intellectual Property Rights (IPR) considerations. A licenseholder could not guarantee FRAND terms including standardization in an accredited SDO with a well-defined IPR policy. That reason was one factor behind CMSAAC not proposing such a solution for geo-targeting. A full review of the IPR issues that were discussed in 2007 would need to be revisited in order to implement ideas related to geo-filtering.

A seemingly necessary condition for device-assisted geo-targeting would be for the device to acquire the coordinates of the polygon. Several techniques below offer different ideas related to the acquisition of the coordinates of the polygon's vertices.

The geo-filtering method described above may continue have IPR protection by one or more entities. Patents have a limited lifetime and a full patent investigation needs to be conducted to evaluate if there are any active patents that may have IPR issues related to geo-filtering.

The proposed ideas which were discussed for enabling a mobile device to perform geo-filtering included:

- Broadcasting Coordinates on Cellular Broadcast Channel
- Downloading Coordinates over WiFi Connection
- Downloading Coordinates over Cellular Data Connection

D.4.1 Broadcasting Coordinates on Cellular Broadcast Channel

Description: Along with broadcasting the text of the WEA Alert Message, the CMSP would also broadcast the coordinates of the alert area. The coordinates could be broadcast in either a concatenated segment, or as separate broadcast message.

Analysis: The table below captures the analysis of this idea:

Table 12: Considerations for Broadcasting Coordinates on Cellular Broadcast Channel

Advantages	Disadvantages
Has the promise of a more precise geo-filtering of alerts. Uses existing WEA broadcast technology. Geo-coordinates would be available for other uses on the mobile device (e.g., display of a personalized map).	Does not apply to devices without GPS capability – differences in level of WEA may impact consumer perception. Continuous operation of GPS on mobile device can drain battery. Processing time may delay rendering of alert, particularly in the absence of needed A-GPS data. Requires the CMSP to use its network resources to broadcast the coordinates in addition to the alert message.

	Legacy mobile devices and feature phones will not be able to support this capability.
Practicality	Practical with some minor challenges: If the coordinates are broadcast in a second message, then there needs to be a way to link the two messages. This requires the development of a standard within 3GPP. Broadcasting the coordinates consumes control channel resources which may complicate the scheduling of when the coordinates are broadcast (and rebroadcast). Devices which rely on MSA-mode A-GPS data may not be able to perform geo-filtering processing. Number of coordinates may exceed the allotted capacity for broadcasting vertices. IPR may pose a legal block or excessive costs to the device manufacturer, OS vendor, and/or CMSP which would likely result in higher cost for handsets to consumers. Calculations of device location are not always 100% accurate and may be subject to error.
Mitigation Options	To conserve broadcast channel resources, broadcast coordinates selectively. If the basic broadcast area is deemed a sufficiently accurate approximation of the target alert area (e.g., in the case of small cells in a dense urban area), then the broadcasting of the coordinates could be omitted. Conversely, if the broadcast area is deemed to contain sufficiently large areas outside the target alert area (e.g., in the case of a macro cell in a rural area), then the coordinates could be broadcast. Further considerations would need to be addressed in the SDOs. If the number of vertices exceeds the allotted capacity, then the polygon could be smoothed by the Alert Originators or according to IPAWS rules and policies. One idea would be to broadcast A-GPS data along with the coordinates. However, this option has not been vetted by experts in the field and will result in more broadcast channel resources required for the WEA broadcast. An alert ID could be included in the bodies of the text message and the vertices message to enable linking of messages (if needed). Consumer perception may be addressed via public outreach.

D.4.2 Downloading Coordinates over WiFi Connection

Description: Upon receiving the WEA Alert Message, the WEA OS app or WEA third party application (TPA) could be programmed to treat it as a trigger to automatically fetch more detailed information, including the alert area's vertices, from a trusted source using the mobile device's WiFi connection. If the mobile is capable of determining its own location, then it could compare its location to the alert area, and render the alert, only if it is located in the alert area. Alternatively, the mobile device could display its location vis-à-vis the alert area. The mobile device could also simply display the alert area on a map.

Analysis: The table below captures the analysis of this idea:

Table 13: Considerations for Downloading Coordinates over WiFi Connection

Advantages	Disadvantages
Has the promise of a more precise geo-filtering of alerts. Does not consume cellular control channel resources for retrieval of additional information required for the geo-targeting.	Does not apply to devices without location determination capability. Continuous operation of GPS and WiFi on mobile device can drain battery. Processing time may delay rendering of alert,

With the typically higher-bandwidth WiFi connection, polygons can have a large number of vertices.	particularly in the absence of needed A-GPS data or availability of a WiFi network. Requires WiFi connectivity: • Not all devices are WiFi enabled. • Not all devices will be in the vicinity of a WiFi network (e.g., in a moving car). Unclear if simultaneous/near-simultaneous requests over WiFi network can bog down the WiFi network. Requires deployment and operation of a "trusted server" to obtain the additional information. Security concerns with obtaining critical alert information over WiFi. Location displays may not be available on feature phones.
Practicality	Practical with some challenges: Issuing a request over a WiFi connection to a server on the Internet requires a mechanism for uniquely identifying the alert in question – in some cases there may be a single active WEA alert, but sometimes there are multiple alerts. Currently WEA Alert Messages do not contain unique alert IDs. The WEA app would need enhanced to automatically determine availability of WiFi connection, and make that connection automatically – the complexity of these steps may vary from device to device, introducing a possible race condition. Requires deployment of a trusted server to obtain additional information on the alert. CMSPs cannot be held liable for anything but what it broadcasts. Calculations of device location are not always 100% accurate and may be subject to error.
Mitigation Options	Alert UID could be virtually created by having the device transmit information such as: • Hash of the alert's text (albeit alert text is not necessarily unique and may result in conflicting information). • ID of the base-station which transmitted the alert – but this would not work as the trusted server would not know the base stations where an alert is broadcast. • The geo-coordinates of the device. WiFi congestion could be mitigated by introducing random delays before sending a request – this would introduce additional delays in rendering the alert to the device, however such additional delays could be tolerable depending on the timescale of the random delays (milliseconds, seconds, etc.)

D.4.3 Downloading Coordinates over Cellular Data Connection

Description: Upon receiving the WEA Alert Message, the WEA OS app or WEA TPA could be programmed to treat it as a trigger to automatically fetch more detailed information, including the alert area's vertices, from a trusted source using the mobile device's cellular data connection (if available). If the mobile device is capable of determining its own location, then it could compare its location to the alert area, and render the alert, only if the device were located in the alert area. Alternatively, the mobile device can display its location vis-à-vis the alert area. The mobile device can also simply display the alert area on a map.

Analysis: The table below captures the analysis of this idea:

Table 14: Considerations for Downloading Coordinates over Cellular Data Connection

Advantages	Disadvantages
Has the promise of more precise geo-filtering of alerts. Technically, does not consume cellular network control channel resources.	Consumes network resources in a most undesired manner i.e., point-to-point communication. Not all devices have cellular data connectivity. Devices that do have cellular data connectivity, could incur data charges which would go against the WARN Act stipulation of no cost to consumers for WEA alerts. Does not apply to devices without location determination capability. Continuous operation of GPS on mobile device can drain battery. Processing time may delay rendering of alert, particularly in the absence of needed A-GPS data.
Practicality	Impractical, given the WEA design decision of no point-to-point communication.
Mitigation Options	Point-to-point communication may be practical if the mobile device is in a (private) Femto cell or a Pico cell, whereby the number of connected devices is limited. However, implementing a system whereby point-to-point communication is allowed in (private) Femto/Pico cells but not in macro cells is not trivial. While the implementation of this mitigation option may make point-to-point WEA communication in Femto/Pico cells practical, the implementation itself (of the mitigation option) is not practical. Further, the CBC currently does not have a method to know whether a cell to which it is broadcasting is in the Macro network or is a Pico/Femto cell.

D.5. Enablers for Device-Oriented Ideas

Note: Some of the enablers in this section have already been mentioned as part of the mitigation options. They are described here in more detail. Also, the enablers in this section may be combined.

The following ideas are described in this section:

- Compression of Geographic Coordinates Data
- Smoothing of Polygon
- Circularization of Polygon
- Embedding of Geographic Data in Text Message

D.5.1 Compression of Geographic Coordinates Data

Description: Geographic coordinates are expressed as latitude and longitude; ISO 6709:2008[28], Standard representation of geographic point location by coordinates, is the international standard for representation of latitude and longitude for geographic point locations. A full latitude/longitude representation (when represented in degrees) has a preceding sign character (-/+), 6 decimal digits for latitude, and 7 decimal digits for longitude

[28] ISO-6709:2008, *Standard representation of geographic point location by coordinates*, Second edition, July 15, 2008; http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=39242.

(±DD.DDDD±DDD.DDDD). Compression of geographic coordinate data allows the representation of the data to be shortened. The type and extent of the compression may affect the accuracy of the data. Various methods may be used to compress the data; for example, since the -/+ sign indicates north or south, east or west on the globe, the signs could be dropped since the mobile device may be able to identify which corner of the globe it is in; or at a minimum it could be assumed that the alert is applicable to a location in USA only. Alternatively, the number of decimal places can be reduced, albeit at the price of reduced precision; it would not be possible for the mobile device to recover the dropped decimal places.

Analysis: The table below captures the analysis of this idea:

Table 15: Considerations for Compression of Geographic Coordinates Data

Advantages		Disadvantages
Reduces the data size (as measured in bits) for representing the polygon's coordinates, making it easier to communicate the coordinates on resource-limited channels as it would allow fitting the information in restricted-size data elements.		In the case of lossy compression, the polygon is distorted, in some case overshooting the original polygon, and in others undershooting the original polygon.
Practicality	Practical with some minor challenges: If compression is performed at the alert origination stage, then alert origination tools would need to be built/upgraded to enable smoothing of polygons.	
Mitigation Options	If compression is performed at the alert origination stage, then any distortion to the original polygon could be visualized for the benefit of the Alert Originator, who could then provide final approval/make necessary modifications to the post-compression polygon.	

Example of a Geocode Compression Technique

Through compression techniques, the Geographic Coordinates Data of the WEA threat area could be packaged to fit into a single LTE packet length of 280 displayable characters. The example below is primarily for illustrative purposes, and other methods for compression are being developed by research sponsored by DHS S&T. The result of this research, along with any other compression techniques, should be considered as part of the ATIS/TIA feasibility study.

In this example, a maximum usable LTE packet length of 280 displayable characters and a polygon shaped alert area is assumed. Using the following method, up to 25 vertices can be broadcast for locations in the northern hemisphere between 100 and 180 degrees west longitude (Figure 13) as well as for Guam in the Eastern hemisphere. Up to 28 vertices can be broadcast in a single packet for locations in the northern hemisphere less than 100 degrees longitude (Figure 14). Up to 23 vertices can be broadcast in a single packet for American Samoa in the southern hemisphere. The format for each latitude/longitude vertex is

(-)LLLL,NNNNN

Where:

- (-)LLLL is latitude in decimal degrees with precision to hundredths (i.e., 2 decimal places). Southern hemisphere values are preceded by a negative sign.

- NNNNN is longitude in decimal degrees with precision to hundredths (i.e., 2 decimal places). Western hemisphere values are between 0 and 180. Eastern hemisphere values are between 500 and 680, where 500 represents 0 degrees east longitude and 680 represents180 degrees east longitude.

Figure 13: Polygon with the following 25 vertices totaling 274 characters. Map drawn using GmapGIS

3445,11826|3443,11833|3439,11838|
3435,11838|3431,11830|3427,11815|
3424,11809|3423,11798|3422,11787|
3421,11782|3420,11774|3417,11770|
3414,11769|3412,11773|3412,11792|
3415,11810|3422,11831|3426,11838|
3429,11845|3433,11849|3437,11852|
3442,11853|3452,11839|3451,11825|
3445,11826

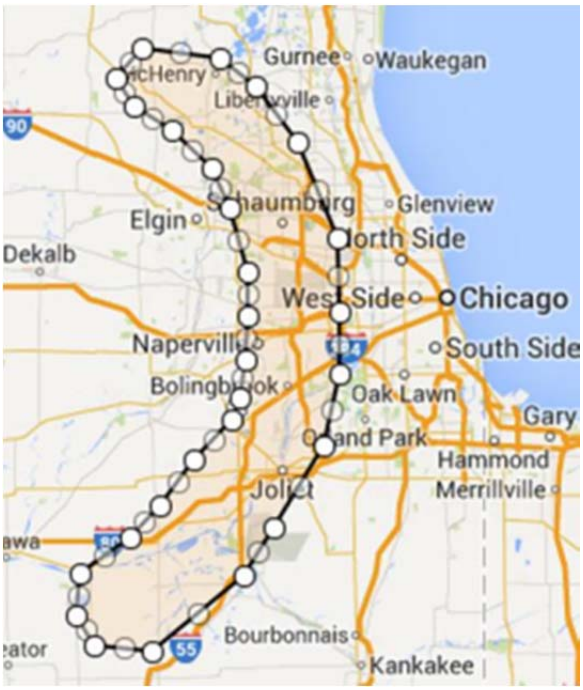


Figure 14: Polygon with the following 28 vertices totaling 279 characters. Map drawn using GmapGIS

4227,8849|4222,8839|4214,8828|
4206,8823|4193,8818|4184,8818|
4175,8818|4167,8820|4163,8822|
4155,8832|4145,8842|4139,8850|
4131,8864|4122,8865|4116,8860|
4115,8844|4131,8819|4141,8810|
4158,8797|4172,8793|4185,8793|
4200,8793|4220,8804|4231,8816|
4237,8826|4239,8847|4233,8854|
4227,8849

D.5.2 Smoothing of Polygon

Description: If the number of vertices of a polygon is too large to be accommodated by whichever mechanism is used to transmit them to the mobile device, the polygon could be smoothed to reduce the number of vertices to an appropriate number. One example of smoothing is to draw a new polygon whereby (a) its number of vertices is smaller than the allowable maximum; (b) it subsumes the original polygon; and (c) it has the least amount area outside the original polygon. There is strong a priori preference for any smoothing of polygons to be performed at the alert origination stage of the WEA system.

Analysis: The table below captures the analysis of this idea:

Table 16: Considerations for Smoothing of Polygon

Advantages	Disadvantages
Reduces the number of lat/long pairs making up the polygon (for example from 30 lat/long pairs to 15 lat/long pairs), thereby reducing the size of the data	The polygon is distorted, likely expanding the original risk area, which in turn may cause devices outside

representing the polygon.	the actual risk area to receive the alert. After the polygon is smoothed, it could result in the same level of geo-targeting precision as what a CMSP is achieving currently via broadcasting. In that case, there is no advantage to this method.
Practicality	Practical with some minor challenges: If smoothing is performed at the alert origination stage, then alert origination tools would need to be built/upgraded to enable smoothing of polygons. The C Interface in the WEA system would need to incorporate any new limits on polygon coordinates. Any modifications to policies or procedures of the C Interface would need to be conducted through the appropriate SDOs.
Mitigation Options	If smoothing is performed at the alert origination stage, then any distortion to the original polygon could be visualized for the benefit of the Alert Originator, who could then provide final approval/make necessary modifications to the smoothed polygon.

D.5.3 Circularization of Polygon

Description: One special case of smoothing is circularization. A circle needs only three parameters: x-coordinate, y-coordinate, and radius. A multi-vertex polygon can be approximated by a circle. There is strong a priori preference for any smoothing of polygons to be performed at the alert origination stage of the WEA system.

Analysis: The table below captures the analysis of this idea:

Table 17: Considerations for Circularization of Polygon

Advantages	Disadvantages
Aggressively reduces the data size (as measured in bits) for representing the polygon's coordinates, making it easier to communicate the coordinates on resource-limited channels as it would allow fitting the information in restricted-size data elements.	The original risk area is expanded by the circle, which in turn may cause devices outside the actual risk area to receive the alert.
Practicality	Practical with some minor challenges: If circularization is performed at the alert origination stage, then alert origination tools would need to be built/upgraded to enable circularization of polygons. If circularization is performed in the FEMA IPAWS, then the FEMA IPAWS system would need to be built/upgraded to enable circularization of polygons.
Mitigation Options	If circularization is performed at the alert origination stage, then the distortion to the original polygon could be visualized for the benefit of the Alert Originator, who could then provide final approval/make necessary modifications to the circle.

D.5.4 Embedding of Geographic Data in Text Message

Description: Characters in the text message could be compressed to reduce the average number of bits per character, allowing for room to add geographic data. A common compression approach is to use fewer bits to represent more common characters, and more bits to represent less common characters. Such an approach can be combined with reducing

the size of the character set (e.g., not allowing foreign characters, using only lowercase or uppercase letters) to further reduce the average number of bits per character.

Analysis: The table below captures the analysis of this idea:

Table 18: Considerations for Embedding of Geographic Data in Text Message

Advantages	Disadvantages
Eliminates the need for the transmission of a second WEA segment containing the coordinates.	Further research is needed to determine the feasibility/potential of this approach. Backward compatibility needs to be managed. Potential for further IPR issues (discussed above), if the compression concepts used are not offered in a FRAND method.
Practicality	TBD based on outcome of research.
Mitigation Options	TBD based on outcome of research.

D.6. Network-Oriented Ideas

As mentioned above, some CMSPs have already made several network-side enhancements to improve WEA geo-targeting e.g., the implementation of polygon based alerting. The subgroup was only able to present one, albeit impractical, new network-oriented idea beyond what has already been implemented. The idea is to perform power-controlled broadcasting, whereby the CMSP could lower the transmission power of an entire base station such that the broadcast reaches a smaller overall area. Since WEA Alert Messages are broadcast on LTE control channels, reducing the broadcast power of the control changes would negatively impact the ability of mobile devices attached with cell site to initiate voice calls including calls to 9-1-1 and Wireless Priority Services (WPS) for Public Safety. Consequently, this idea is not a practical solution without negatively impacting emergency services, public safety, and the general communications capabilities of the subscribers. The concept is illustrated in Figure 15 below, which attempts to illustrate a case where power control would work.

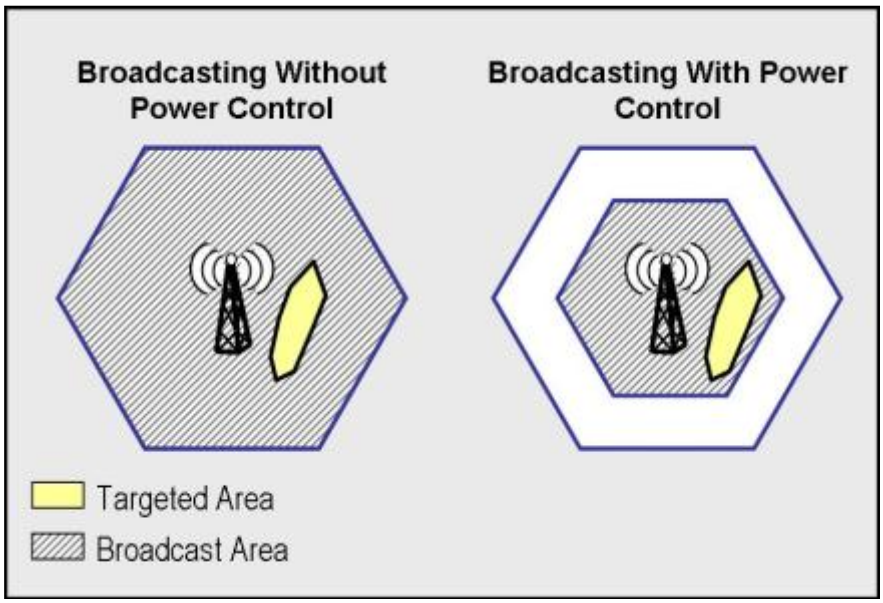


Figure 15: Illustration of Geo-Targeting Enhancement via Power Control

The table below contains the analysis of this idea:

Table 19: Considerations for Geo-Targeting Enhancement via Power Control

Advantages	Disadvantages
Applies equally to all mobile devices in network regardless of the technological capabilities of the device. Could be phased in incrementally over time after standardization.	Degree of enhancement depends on location of alert area relative to cellular tower – the closer it is to the cellular tower the larger the impact of the enhancement. This power control option reduces the CMSP's coverage area for voice and data services for the duration of the alert (which, during an Amber alert can be as long as 23 hours), creating coverage holes and denying service to its customers including the ability of subscribers to make emergency calls to 9-1-1 and the ability of Public Safety to use Wireless Priority Services (WPS) for communications access under emergency conditions.
Practicality	Not Practical: WEA Alert Messages are broadcast on the control channel. Current standards for cellular networks do not support real-time adjustment of the power level of the control channel. Re-designing cellular networks to support power-controlled control channels requires a re-architecture of the global LTE system, global standardization, and updates to the global LTE implementations.
Mitigation Options	None.

D.7. Approaches Based on Third-Party Assistance

This approach is third-party-assisted enhancements. For example, upon receiving the WEA Alert Message, a mobile-device may send a "should-display?" request to a third party service over the Internet. The third-party service may be able to determine the location of the mobile device and respond with a "Yes/No" response.

Note: The third-party assistance may need to rely on assistance from the CMSP [e.g., CMSP's Commercial Location Based Services (LBS)].

The third-party-assisted geo-targeting techniques are outside the scope of this report.

Appendix E: Geo-targeting Analysis

This Appendix provides some examples of alert broadcasting scenarios with more emphasis on the geo-targeting aspects.

For the purpose of illustration, this Appendix introduces the terms such as Warning Area, Alert Area, Broadcast Area, and Desired Area. Warning Area is the actual area to which WEA is in effect. Desired area is the list of cell-sectors affected due to the WEA. Alert area is the area specified by the Alert Originator as WEA affected area. Broadcast area is the area to which the alert is broadcast by the CMSP.

E.1. Background

Also for the purpose of illustration, a hypothetical region consisting of two counties (named County A and County B) are considered (see Figure 16 below), and in the subsequent examples illustrated in this Appendix, and a WEA affects users of these two counties. For the purpose of illustration, a cell-sector is considered to be within the county if a part of that cell-sector belongs to the county. In example shown in Figure 16, some cell-sectors may be part of two counties.

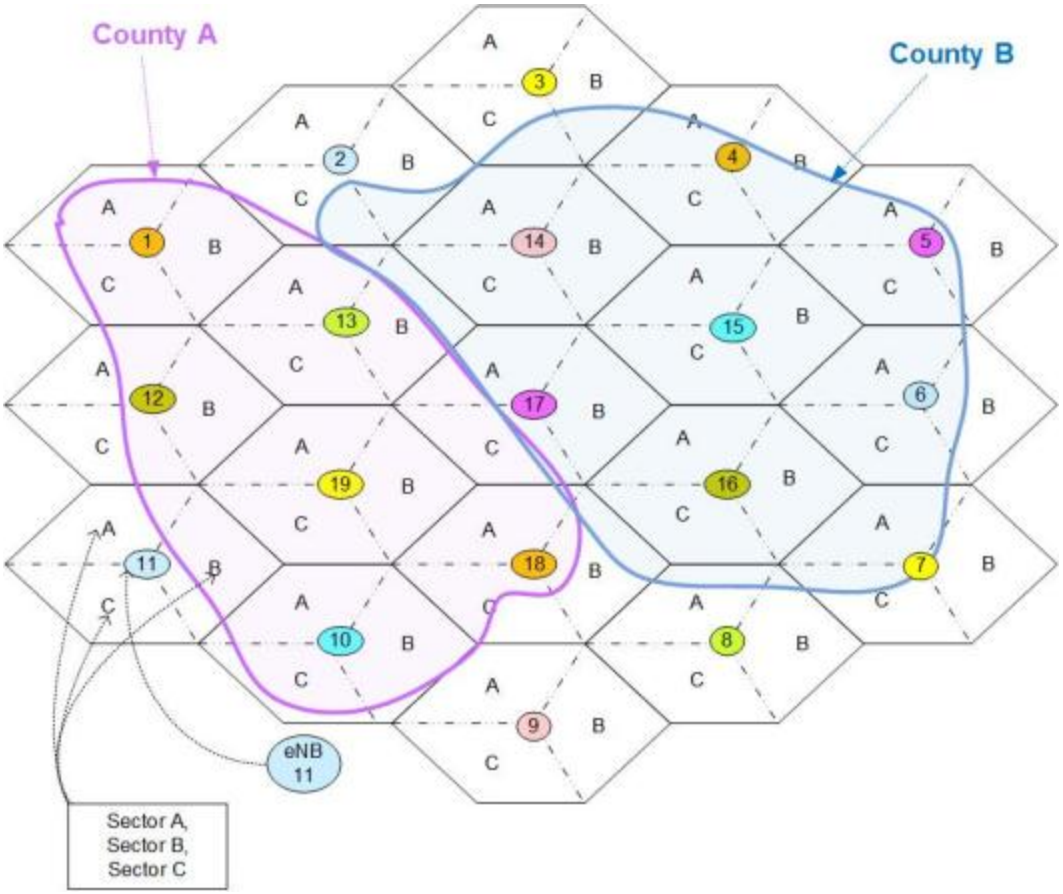


Figure 16: Hypothetical Region Consisting of Two Counties - County A and County B

The Figure 16 shows 19 eNBs, each with 3 sectors identified as A, B and C. The cell-sectors that belong to County A and County B are shown in Table 20.

Table 20: Cell-Sectors in County A and County B

County A	
eNB	Cell-Sectors
1	A*, B*, C*
2	C*
10	A*, B*, C*
11	A*, B*
12	A*, B, C*
13	A*, B*, C
17	A*, C*
18	A*, B*, C*
19	A, B, C

County B	
eNB	Cell-Sectors
2	B*, C*
3	B*, C*
4	A*, B*, C
5	A*, B*, C*
6	A*, B*, C*
7	A*, B*, C*
8	A*, B*
13	A*, B*
14	A, B, C
15	A, B, C
16	A, B, C
17	A*, B, C*
18	A*, B*

Note: A "*" next to the cell-sector (e.g., A*) indicates that only a part of the cell-sector lies within the indicated county boundary.

In this illustration, as can be seen in Figure 16, the following cell-sectors are outside the two county boundaries:

- eNB 2, cell-sector A
- eNB 3, cell-sector A
- eNB 8, cell-sector C
- eNB 9, all three cell-sectors
- eNB 11, cell-sector C

The methods used to determine the Alert Area and Broadcast Area in the current geo-targeting method are described in Section 3.2. This illustration takes only a part of those variables.

E.1.1 Warning Area

Figure 17 shows an example where a WEA is affecting the users of two counties as shown in Figure 16. The red-shaded area with the solid red lines is the Warning Area.

Even though the Warning Area appears to be polygon, the Alert Originators may choose the entire county, or a part of the county as an Alert Area. Or, alternatively, the Alert Originators may provide the coordinates of the polygon to identify the Alert Area. Other possible methods are not included in this illustration.

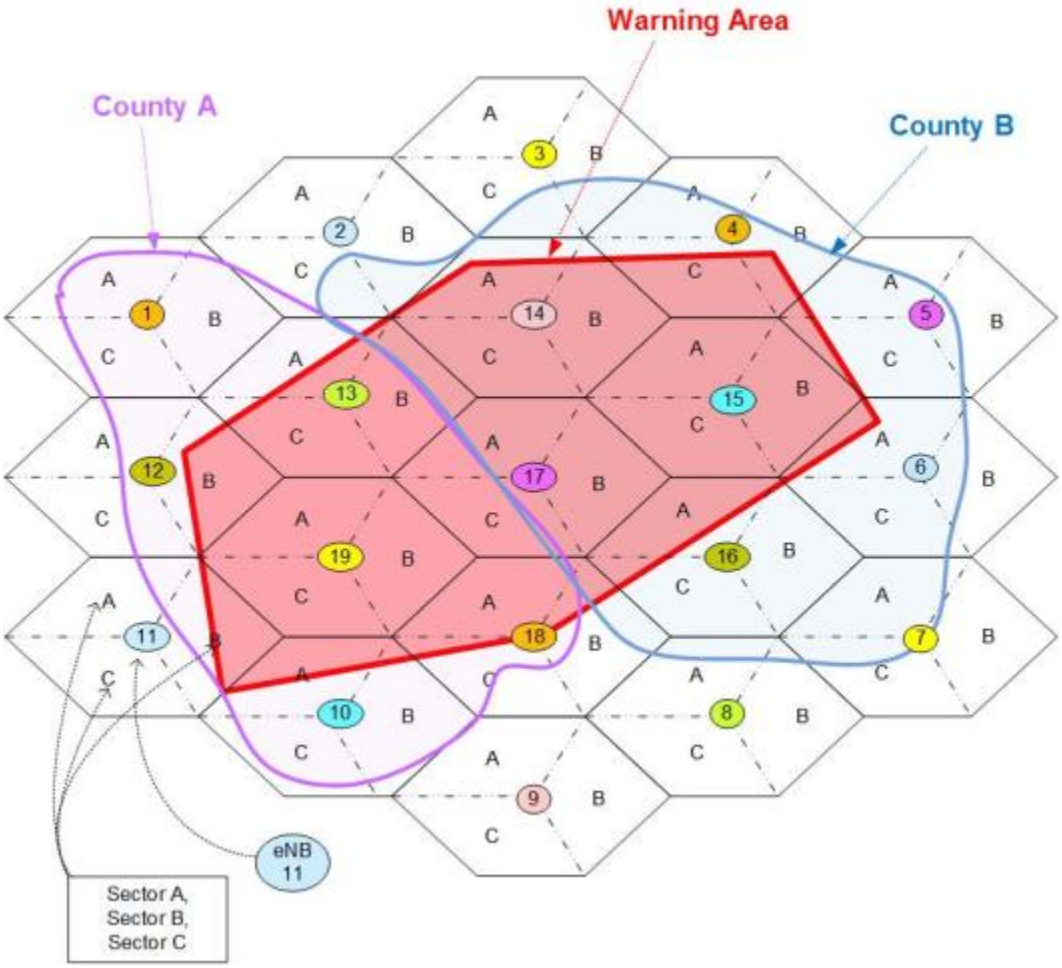


Figure 17: Warning Area Affecting Users of Two Counties

The cell-sectors that belong to the Warning Area are shown in Table 21.

Table 21: Cell-Sectors in Warning Area

eNB	Cell-Sector
4	B*, C*
5	A*, C*
6	A*, C*
10	A*, B*
11	B*
12	B*
13	A*, B, C*
14	A*, B*, C
15	A, B, C
16	A*, B*, C*
17	A, B, C
18	A, B*, C*
19	A, B, C

Note: A "*" next to the cell-sector (e.g., A*) indicates that only a part of the cell-sector lies within the Warning Area.

E.1.2 Desired Area

Since a WEA cannot be broadcast to part of a cell-sector, all users within a cell-sector receive the WEA if at least a part of that cell-sector lies within Warning Area boundary. Figure 18 shows the Desired Area as compared to the Warning Area shown in Figure 17.

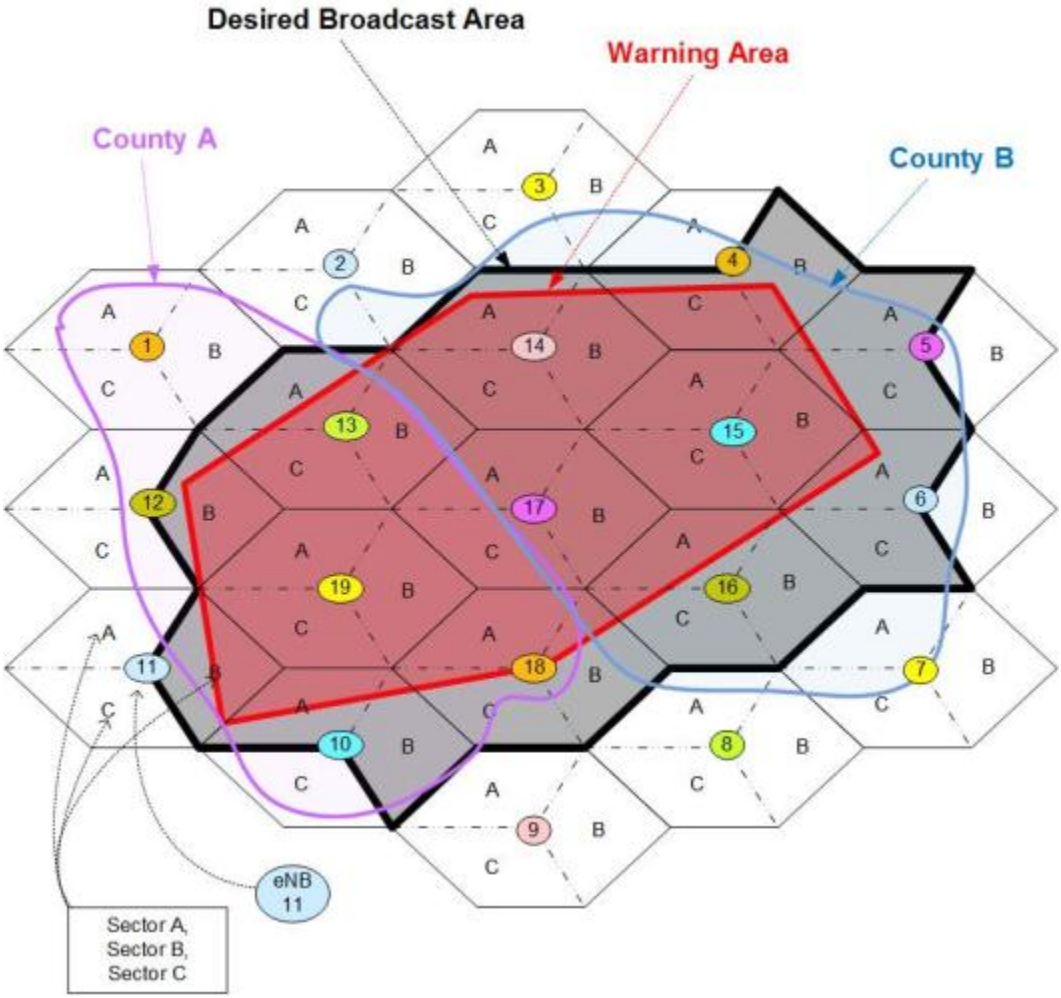


Figure 18: Desired Area for WEA Broadcast

The cell-sectors that belong to the Desired Area are shown in Table 22.

Table 22: Cell-Sector in Desired Area

eNB	Cell-Sector
4	B, C
5	A, C
6	A, C
10	A, B

eNB	Cell-Sector
11	B
12	B
13	A, B, C
14	A, B, C
15	A, B, C
16	A, B, C
17	A, B, C
18	A, B, C
19	A, B, C

Note: The cell-sectors in the Desired Area are same as the cell-sectors in the Warning Area except that the entire cell-sector is included in the Desired Area.

This illustration uses the entire cell-sector for the broadcast if a part of the cell-sector is within the Warning Area. That is why the Desired Area appears to be larger than the Warning Area. Also, the concept of Desired Area is for illustration purpose only and as such it does not come into the picture of WEA broadcast.

E.2. Alert Area and Broadcast Area

The examples shown here consider the following cases:

- Alert area is identified based on county boundary
- Alert area is identified based on a polygon
- Broadcast area based on the physical location of eNB
- Broadcast area based on the geographical centroid of the sector.

As explained earlier, Alert Area may be identified through other means as described in Section 3.2.1.1 and Broadcast Area may also be performed through other means described in Section 3.2.1.2. But, the purpose of this Appendix is to give a general idea and therefore, the illustration is limited to the above bulleted cases.

E.2.1 Alert Area at County Level

In this case, the entire county is identified as Alert Area. So, CMSP would distribute the alert to the entire county. The Broadcast Area can be determined based on the physical location of the eNB or the geographical centroid of the cell-sector. Each case is illustrated below.

Broadcast Area Based on eNB Physical Location

An eNB is considered to be within the Broadcast Area if the physical location of that eNB is within the county (i.e., Alert Area). Figure 19 illustrates the Broadcast Area for the Warning Area shown in Figure 17.

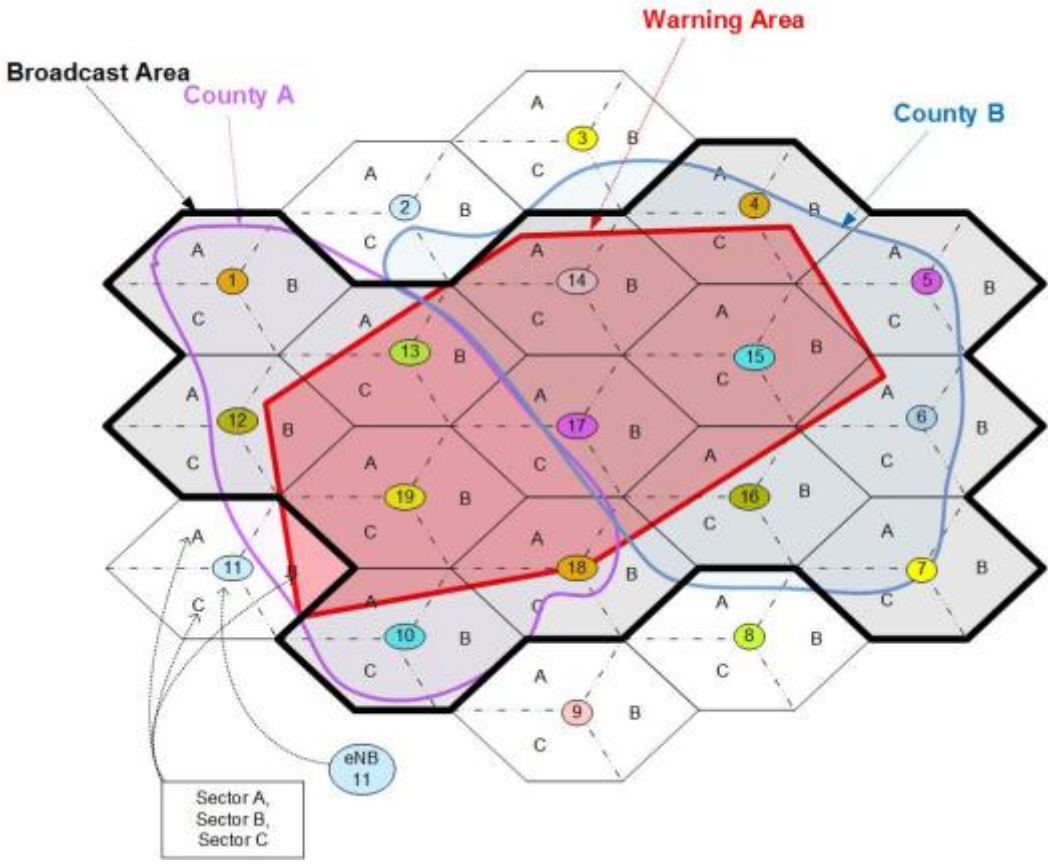


Figure 19: Broadcast Area Determined Based eNB Location

Based on Figure 19, the Table 23 is constructed to identify the cell-sectors that belong to the Broadcast Area.

Table 23: Cell-Sectors in Broadcast Area

eNB	Cell-Sector
1	A, B, C
4	A, B, C
5	A, B, C
6	A, B, C
7	A, B, C
10	A, B, C
12	A, B, C
13	A, B, C
14	A, B, C
15	A, B, C
16	A, B, C
17	A, B, C
18	A, B, C
19	A, B, C

Certain users within the county may not receive the WEA because the physical location of the eNB is outside of the county boundary.

Broadcast Area Based on Geographical Centroid of The Cell-Sector

A cell-sector is considered to be within the Broadcast Area if the geographic centroid of the cell-sector is in within the county. Figure 20 illustrates the Broadcast Area for the Warning Area shown in Figure 17.

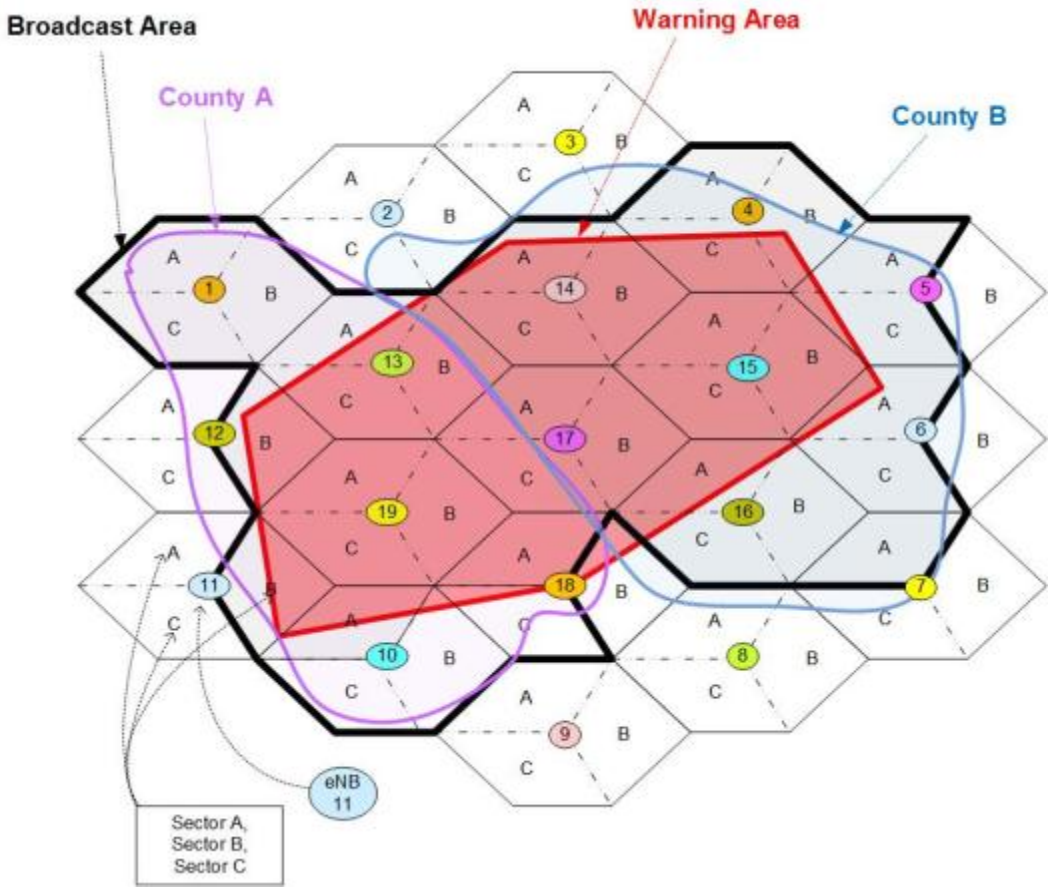


Figure 20: Broadcast Area Determined Based Cell-Sector Centroid Location

Based on Figure 20, the Table 24 is constructed to identify the cell-sectors that belong to the Broadcast Area.

Table 24: Cell-Sectors in Broadcast Area

eNB	Cell-Sector
1	A, B, C
4	A, B, C
5	A, C
6	A, C
7	A

eNB	Cell-Sector
10	A, B, C
11	B
12	B
13	A, B, C
14	A, B, C
15	A, B, C
16	A, B, C
17	A, B, C
18	A, C
19	A, B, C

Certain users within the county may not receive the WEA because the geographical centroid of the cell-sector they are in is outside of the county boundary.

Comparison

The Figure 21 gives an overview of the Desired Area to the Broadcast Area associated with the two approaches.

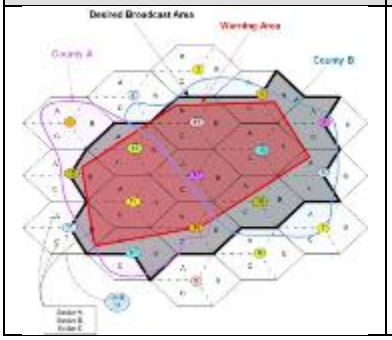
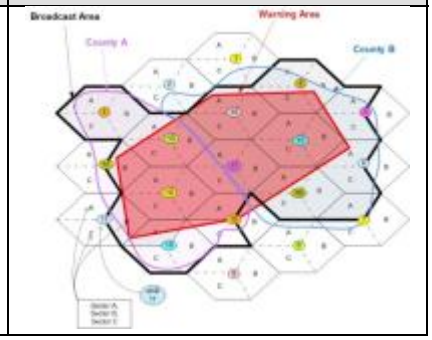
Desired Area	Broadcast Area	
	With eNB Location	With Cell-Sector Centroid
		

Figure 21: County Level Alert Area Comparison

Table 25 below compares the cell-sectors of the Broadcast Area with the Desired Area.

Table 25: Cell-Sectors in Warning Area, Desired Area and Broadcast Area

eNB	Cell-Sectors			
	Warning Area	Desired Area	Broadcast Area	
			eNB	Cell-Sector
1			A, B, C	A, B, C
4	B*, C*	B, C	A, B, C	A, B, C
5	A*, C*	A, C	A, B, C	A, C
6	A*, C*	A, C	A, B, C	A, C
7			A, B, C	A
10	A*, B*	A, B	A, B, C	A, B, C

eNB	Cell-Sectors			
	Warning Area	Desired Area	Broadcast Area	
			eNB	Cell-Sector
11	B*	B		B
12	B*	B	A, B, C	B
13	A*, B, C*	A, B, C	A, B, C	A, B, C
14	A*, B*, C	A, B, C	A, B, C	A, B, C
15	A, B, C	A, B, C	A, B, C	A, B, C
16	A*, B*, C*	A, B, C	A, B, C	A, B, C
17	A, B, C	A, B, C	A, B, C	A, B, C
18	A, B*, C*	A, B, C	A, B, C	A, C
19	A, B, C	A, B, C	A, B, C	A, B, C

Note: A "*" next to the cell-sector (e.g., A*) indicates that only a part of the cell-sector lies within the Warning Area. The cell-sectors in the Desired Area are same as the cell-sectors in the Warning Area except that the entire cell-sector is included in the Desired Area. Broadcast area is determined if the physical location of the eNB or the centroid of the cell-sector is in the county A or County B because Alert Area specified by the Alert Originator is at a county-level.

Looking at the Table 25, it can be seen that Broadcast Area is different from the Desired Area. With the eNB location being used to determine the Broadcast Area, the WEA is broadcast to about 39% more cell-sectors than the desired number of cell-sectors and about 3% less cell-sectors than the desired number of cell-sectors. With centroid of the cell-sector being used to determine the Broadcast Area, WEA is broadcast about 19% cell-sectors more than the desired number of cell-sectors and 3% less than the desired number of cell-sectors. With eNB-based method, users served by the cell-sector B of eNB-11 do not receive the WEA. With centroid of the cell-sector based method, users served by the cell-sector B of eNB-18 do not receive the WEA.

E.2.2 Alert Area Polygon

In this case, the Alert Area is identified with a polygon. For purpose of this illustration, in this case, the Alert Area and Warning Area are one and the same because Warning Area shown in Figure 17 is also a polygon. CMSP would distribute the alert to the cells that are in the polygon. The Broadcast Area can be based on the physical location of the eNB or the geographical centroid of the sector. Each case is illustrated below.

Broadcast Area Based on eNB Physical Location

An eNB is considered to be within the Broadcast Area if the physical location of that eNB is within the polygon (i.e., Alert Area). The Figure 22 illustrates the Broadcast Area for the Warning Area shown in Figure 17.

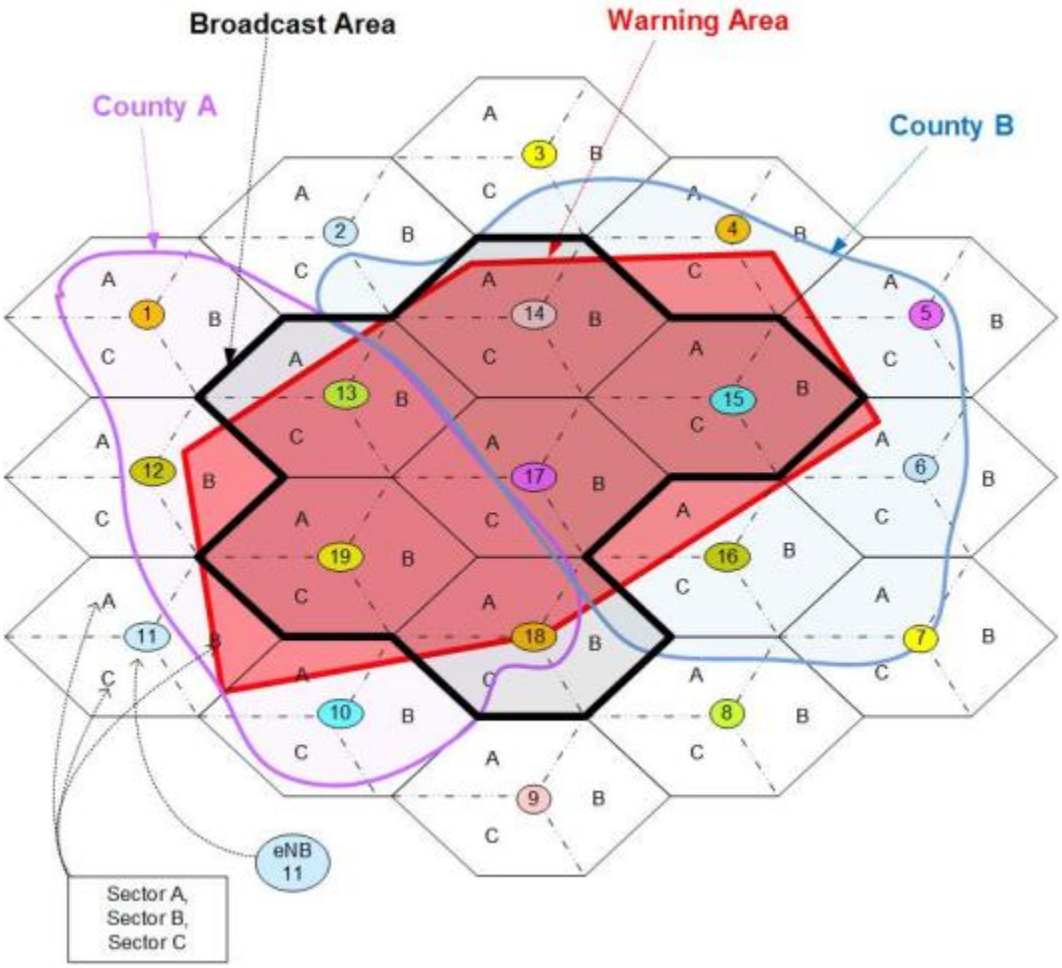


Figure 22: Broadcast Area Determined Based eNB Location

Based on Figure 22, the Table 26 is constructed to identify the cell-sectors that belong to the Broadcast Area.

Table 26: Cell-Sectors in Broadcast Area

eNB	Cell-Sector
13	A, B, C
14	A, B, C
15	A, B, C
17	A, B, C
18	A, B, C
19	A, B, C

Broadcast Area Based on Geographical Centroid of The Cell-Sector

A cell-sector is considered to be within the Broadcast Area if the geographic centroid of the cell-sector is within the polygon. The Figure 23 illustrates the Broadcast Area for the Warning Area shown in Figure 17.

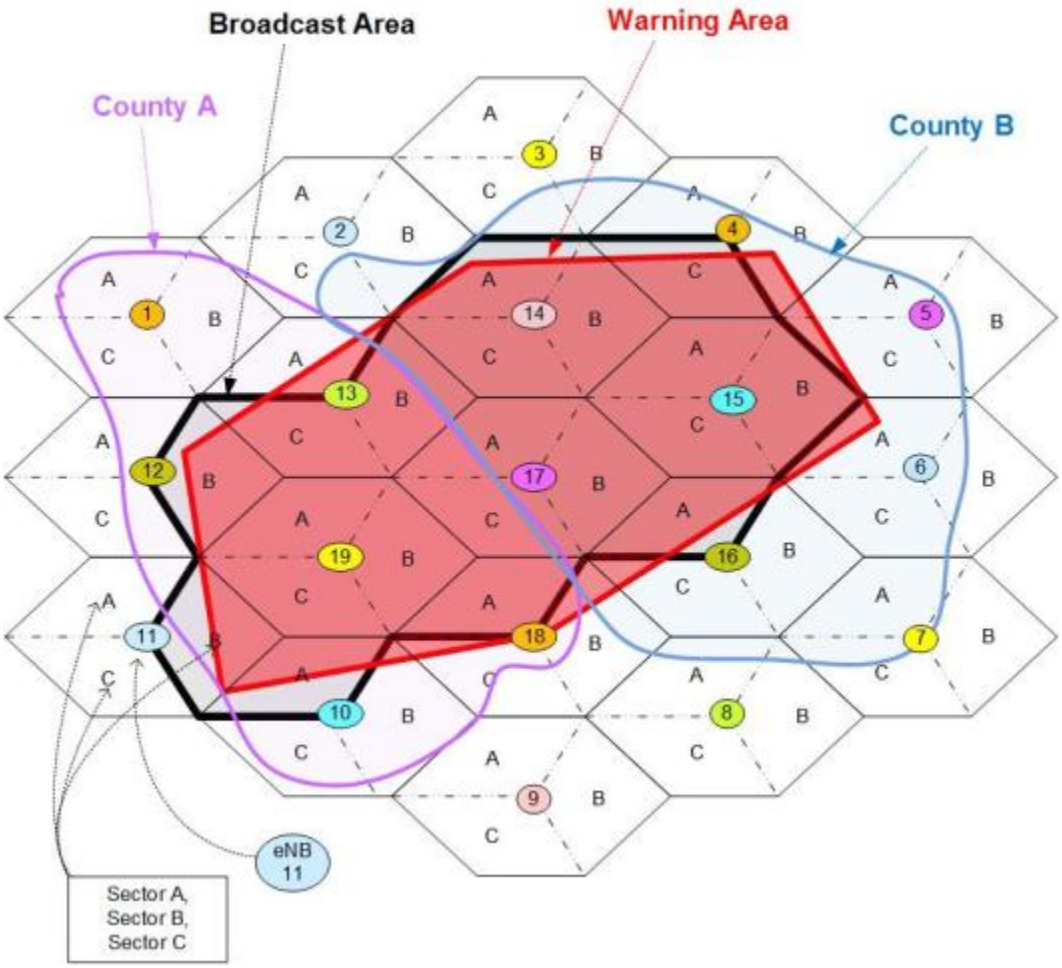


Figure 23: Broadcast Area Determined Based Cell-Sector Centroid Location

Based on Figure 23, the Table 27 is constructed to identify the cell-sectors that belong to the Broadcast Area.

Table 27: Cell-Sectors in Broadcast Area

eNB	Cell-Sector
4	C
10	A
11	B
12	B
13	B, C
14	A, B, C
15	A, B, C
16	A
17	A, B, C
18	A
19	A, B, C

Comparison

The Figure 24 gives an overview of the Desired Area to the Broadcast Area associated with the two approaches.

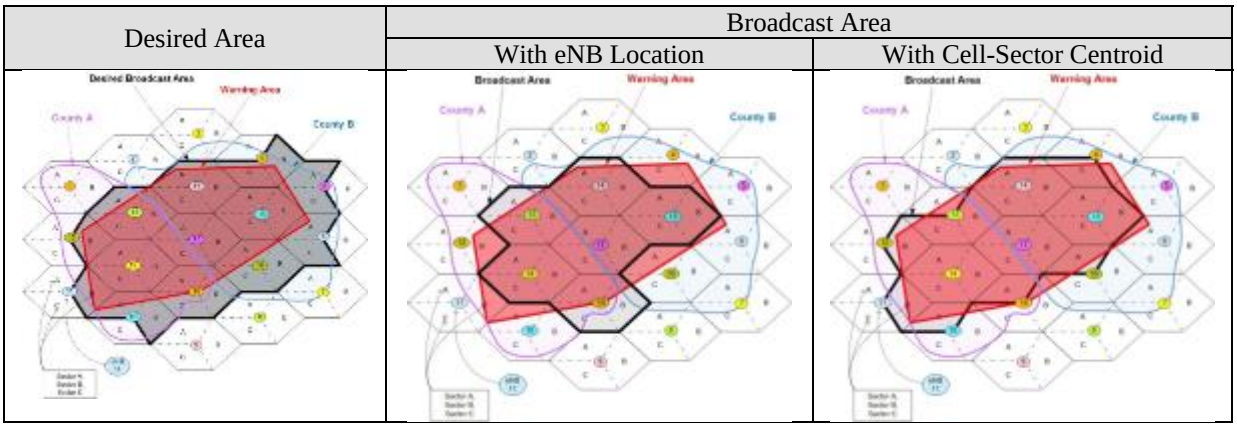


Figure 24: Polygon Alert Area Comparison

The Table 28 below compares the cell-sectors of the Broadcast Area with the Desired Area.

Table 28: Cell-Sectors in Warning Area, Desired Area and Broadcast Area

eNB	Cell-Sectors			
	Warning Area	Desired Area	Broadcast Area	
			eNB	Cell-Sector
1				
4	B*, C*	B, C		C
5	A*, C*	A, C		
6	A*, C*	A, C		
7				
10	A*, B*	A, B		A
11	B*	B		B
12	B*	B		B
13	A*, B, C*	A, B, C	A, B, C	B, C
14	A*, B*, C	A, B, C	A, B, C	A, B, C
15	A, B, C	A, B, C	A, B, C	A, B, C
16	A*, B*, C*	A, B, C		A
17	A, B, C	A, B, C	A, B, C	A, B, C
18	A, B*, C*	A, B, C	A, B, C	A
19	A, B, C	A, B, C	A, B, C	A, B, C

Note: A "*" next to the cell-sector (e.g., A*) indicates that only a part of the cell-sector lies within the Warning Area. The cell-sectors in the Desired Area are same as the cell-sectors in the Warning Area except that the entire cell-sector is included in the Desired Area. Broadcast area is determined if the physical location of the eNB or the centroid of the cell-sector is in the polygon because Alert Area specified by the

Alert Originator as a polygon.

Looking at the Table 28, one can see that Broadcast Area is different from the Desired Area. With the eNB location being used to determine the Broadcast Area, the WEA is broadcast to about 42% less cell-sectors than the desired number of cell-sectors. With centroid of the cell-sector being used to determine the Broadcast Area, WEA is broadcast about 35% cell-sectors less than the desired number of cell-sectors. With eNB-based method, users served by the cell-sector B of eNB-11 do not receive the WEA.

Appendix F: Future Mobile Alerting Concept

Executive Order 13407 – Public Alert and Warning System[29] states "It is 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". Recent natural disasters such as Hurricane Katrina and Sandy as well as the terrorist attacks in New York City and Boston underscore the need for redundancy and reliability in our warning networks so that people may be alerted wherever they may be or for whatever situation they may be in.

While WEA is and should remain a voluntary service which places obligations on Participating Commercial Mobile Service Providers, this idea goes beyond WEA which includes non-WEA components in a more comprehensive concept. The advancement of communication technologies in mobile devices is evolving towards 5G, and additional capabilities may be difficult to predict. The communication capabilities of mobile devices can only be expected to continue to advance in the coming years. These capabilities could be used to provide additional reliability and redundancy beyond WEA particularly in light of any natural or manmade disaster that damages, partially or in whole, our terrestrial communications networks.

The future mobile alerting concept is for the mobile device to receive alert information from FEMA IPAWS over multiple transmission channels that may be available in the mobile device, to capitalize on the capabilities and attributes of each transmission channel to reach devices in the defined alert area. Devices under this concept may include cell phones, automobiles, computers or any device with communications access, a display screen, and location based technology.

The concept is analogous to EAS where the message is broadcast over multiple channels (i.e., EAS tones from NOAA Weather Radio and CAP EAS from FEMA IPAWS), but only one of the sources is used by the receiving device and the duplicate is automatically ignored. The alert message, along with geo-coordinates of the actual alert area to assist with geo-targeting, is transmitted to the mobile device over all available communication channels equipped on the mobile device. These channels may include cellular (LTE or future 5th generation) broadcast, WiFi, cellular data (if enabled by end-user), satellite (if mobile device is equipped with satellite receiver) and future broadcast technologies.

- In the case of cellular data and WiFi, the alert message is pushed to the mobile device from a trusted server, which itself receives the alert message and related information from the FEMA IPAWS alert aggregator.
- In the case of cellular systems (LTE or future 5th generation), the alert message is sent using WEA.
- In the case of satellite transmission, a satellite provider receives the alert information from FEMA IPAWS with the server possibly acting as a gateway with the satellite provider. The satellite provider may perform an initial mapping of the alert area to the

[29] Executive Order 13407 – Public Alert and Warning System, signed June 26, 2006 by President George W. Bush. http://www.gpo.gov/fdsys/pkg/WCPD-2006-07-03/pdf/WCPD-2006-07-03-Pg1226.pdf. Note: This Executive Order was published in the Federal Register on June 28 2006.

satellite coverage that best matches the alert area.

- In the case of future broadcast technologies, the alert is sent from FEMA IPAWS to the broadcast provider who broadcasts the alert to an area that best matches the alert area.

Upon receipt of the alert, the mobile device renders the alert and ignores duplicates which arrive via other channels. Additional information included in subsequent alerts can also be shared with the user to give them more information about the alert. The mobile device should be capable of using current and future broadcast technologies as well as leveraging the intelligence contained in devices as devices evolve in the marketplace.

Table 29: Considerations for Future Mobile Alerting Concept

Maximum Length			Would have to be determined via a standardization process between the wireless operators, DHS S&T, FEMA and the alert originator community.
Existing WEA Elements & Interfaces	**EOC**	**Alert Originator**	In order to accommodate existing base of WEA-enabled mobile devices, as well as mobile devices capable of receiving longer messages, the Alert Originator needs to create two WEA Alert Messages, the first adhering to the 90-char max and the second to the longer max.
		Alert Origination Tool	The Alert Originator Tool will need to create the more detailed information for the trusted source.
	FEMA IPAWS	**Aggregator**	FEMA IPAWS will need modifications to receive from the alert originator the more detailed information to the trusted source whenever a WEA Alert Message is sent to the wireless operators. Modifications to the FEMA IPAWS would be required to support receiving the information from the alert originator to be sent to the trusted source.
		Gateway	FEMA IPAWS will need modifications to receive the larger message and to support and/or deliver the more detailed information to the trusted source whenever a WEA Alert Message is sent to the wireless operators.
	CMSP	**Gateway**	If a different message ID is used, modifications are required to the 3GPP standards to also support the longer WEA Alert Messages and to support inbound international roamers. If a different message ID is used, modifications to the CMSP WEA infrastructure would be required. Modifications required to Joint ATIS/TIA CMAS standards for C-Interface and C-Interface testing.
		Core Network and Radio Elements	None – this assumes a standard WEA Alert Message will be used. If a different cell broadcast message ID is used to differentiate this capability, modifications are required to the 3GPP standards to also support the new message id and to support inbound international roamers.
		Mobile Device	New mobile devices are required to support the ability to access the more detailed information when a WEA Alert Message is received. Modifications required to Joint ATIS/TIA CMAS standards for

			mobile device behavior. Native WEA OS App needs to expose the WEA Alert Message to third-party apps or WEA OS App.
	Interfaces	**A**	CAP message needs to support the longer WEA Alert Message with indication of the trusted source.
		B	CAP message needs to support the longer WEA Alert Message with indication of the trusted source.
		C	Modifications to the C interface would be required to support the longer WEA Alert Message with indication of the trusted source.
		D	If a different message ID is used, modifications to the CMSP WEA infrastructure would be required.
		E	If a different message ID is used, modifications would be required to the 3GPP standards to also support the longer WEA Alert Messages and to support inbound international roamers.
Non-WEA Elements	**CMSP**	**WiFi**	The WEA app on the mobile device would need to establish a WiFi connection with the trusted server to retrieve the additional information.
		Data Session Satellite Broadcast Technologies	None.
Implications for Mobile Device app Enhancements			One implementation option is to have a mobile app with the intelligence to execute method as described. Would need changes to mobile device functionality to support this alternative and any mobile device app implementation options.
Trusted Server			One implementation option is provide information to mobile device app upon request in a secure, reliable and scalable fashion. May also need to be connected to IPAWS OPEN; security may be problematic for untrusted mobile devices connecting to IPAWS directly. For non broadcast channels, need to provide information to third-party WEA app a secure, reliable and scalable fashion, whereby the information needs to be delivered to the mobile app on a push basis. Needs to have a direct connection to FEMA IPAWS.
Pros			Supports longer WEA Alert Messages for mobile devices which have active alternative connections. Use of WiFi does not disrupt the cellular network. Creates redundant distribution of the alert to reach nearly all devices within the alert area. Removes repetitive alerting of the device for the same alert. Broadcast channels such as LTE cell broadcast, eMBMS and satellite have ability to reach devices within their broadcast area. Satellite coverage includes the entire country and territorial

	waters and can deliver alerts even when the terrestrial system is compromised due to natural or man made disasters. Using location of the device as a filter to display the alert, geo-fences the alert to the polygon created by the alert originator no matter what channel delivers the alert to the device. Multiple delivery channels leverages the different payload and service capabilities of each channel to enhance reliability and resilience. WiFi and Broadcast technologies compliment the wireless network. The mobile device, using multiple delivery channels, provides uniformity of the alert to the device.
Cons	Unlike capabilities in the CMSP infrastructure which target supporting all users and devices, older devices may not have access to all the new capabilities of this future alert system. This is suggesting an extremely complex and complicated end user mobile device which is not required for the subscriber's basic telecommunication services. It is not envisioned that devices described here (e.g., satellite capable) due to the inherent cost and complexities. It is especially true since underlying CMSP infrastructure can support longer messages. This option places obligations on satellite providers in addition to CMSPs. Satellite provider obligations are under EAS and not WEA which would complicate the rules. This option would require a international standardization and best practices efforts encompassing both wireless technologies and satellite technologies. This option would coordination between alert originators, FEMA IPAWS, CMSPs, and satellite providers. Note: no satellite providers are represented on this CSRIC IV working group. This option assumes that satellite providers perform beam spotting but this may not be a valid assumption. There is no information in the WEA text message to correlate it to the original alert message. Use of a different message ID to provide the information on the location of the information on the trusted server would need development efforts for the CMSP infrastructure. Support of a different message ID to provide the information on the location of the information on the trusted server also requires mobile device modifications. This option will require new mobile device designs which could be complex and costly. If new mobile device chipsets are required, the development could take several years and would take even longer to be distributed to end users. It cannot be assumed that mobile devices are connected to WiFi. • Mobile devices may not automatically connect to WiFi without some other type of user intervention. • Not every mobile device may have WiFi capabilities. • Subscriber may have turned off the WiFi connection.

	• Subscriber may not have configured WiFi connections. • WiFi connections generally not available in rural and remote locations. • WiFi connections may not be available in suburban locations beyond subscriber's home or neighborhood stores (e.g., coffee shop). • If driving in a car, the mobile device may be connected to WiFi within the car but the car is not WiFi connected to external access points. • WiFi connections may not be free and the subscriber may not be subscribed to the WiFi service. • Network congestion of WiFi connections may occur. The trusted server may be overloaded. The alternative must scale for potential nationwide alerts covering 300+ million mobile devices. There are no mobile device APIs defined for third party apps to receive the information. This option assumes a particular implementation in the mobile device. At least one smartphone OS does not store the WEA Alert Messages in a WEA inbox. Therefore, it will not be possible for a WEA app to retrieve that alert message on that smartphone OS. An entity has to be identification established to be the "trusted source" The trusted source would need to open their systems to every mobile device in the world with no security mechanisms. It can be envisioned that malware or man-in-the-middle attacks could be used to cause havoc. Even though a larger number of displayable characters can be broadcast, the form factors of various types and models of mobile devices to not easily facilitate the presentation of very large alert messages.
Challenges with Regard to WARN Act	This alternative has potential conflicts with the WARN Act requirements, which should be investigated. Obligations on Participating CMSPs and other communications providers need to be addressed. The Participating CMS provider is not responsible for the trusted source or retrieval process. This alternative is beyond the obligations of the CMSPs.
Mitigating Factors	Some users may seek additional information on their own. There may be potentially many sources of information to which they can turn. There are techniques available to handle potential overloading of trusted servers. Content staging and load balancing are examples of potential mitigations for the overloading of trusted server. To correlate the message at the trusted server with the WEA alert, additional information must be provided in the WEA Alert Message. Additional study is required to evaluate the

	character limitations and capabilities available in LTE. The satellite industry standards body would be needed to evaluate this alternative and provide any mitigating factors to the impacts to the satellite networks.

Appendix G: Acronyms

This Appendix contains the acronyms that are referenced within this report.

Acronym	Definition
2G	Second Generation
3G	Third Generation
3GPP	3rd Generation Partner Project
3GPP2	3rd Generation Partnership Project 2
4G	Fourth Generation
A-GPS	Assisted GPS
API	Application Programming Interface
ATIS	Alliance for Telecommunications Industry Solutions
bps	Bits per second
CAP	Common Alerting Protocol
CBC	Cell Broadcast Center
CBE	Cell Broadcast Entity
CBS	Cell Broadcast Service
CDMA	Code Division Multiple Access
CFR	Code of Federal Regulations
CMAS	Commercial Mobile Alert Service
CMS	Commercial Mobile Service
CMSAAC	Commercial Mobile Service Alert Advisory Committee
CMSP	Commercial Mobile Service Provider
COE	Center of Excellence
CSRIC	Communications Security, Reliability and Interoperability Council
CTIA	Cellular Telecommunications Industry Association
DHS	Department of Homeland Security
DHS S&T	Department of Homeland Security Science and Technology Directorate
EIA	Electronic Industries Alliance
eMBMS	enhanced Multimedia Broadcast Multicast Service
eNB	Evolved Node B
EOC	Emergency Operations Center
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
FRAND	Fair, Reasonable and Non-Discriminatory

Acronym	Definition
GNIS	Geographic Names Information System
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GW	Gateway
IPAWS	Integrated Public Alert and Warning System
IPR	Intellectual Property Rights
kB	kilobyte
LBS	Location Based Services
LCS	Location Services
LTE	Long Term Evolution
MHz	Megahertz
MI	Message Identifier
MSA	Mobile Station Assisted
MSB	Mobile Station Based
NWS	National Weather Service
OASIS	Organization for the Advancement of Structured Information Standards
PWS	Public Warning System
RDT&E	Research, development, testing and evaluation
RF	Radio Frequency
S-GPS	Standalone/autonomous GPS
SAME	Specific Area Message Encoding
SDO	Standards Development Organization
SIB	SystemInformationBlock
SIB12	SystemInformationBlockType12
SOW	Statement of Work
SSID	Service Set Identification
START	Study of Terrorism and Responses to Terrorism
TBD	To Be Determined
TIA	Telecommunications Industry Association
TPA	Third Party Application
UID	User Identifier
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
USGS	United States Geological Survey
WARN	Warning, Alert, and Response Network

Acronym	Definition
WCDMA	Wideband CDMA
WEA	Wireless Emergency Alerts
WG	Working Group
WPS	Wireless Priority Service

Appendix H: Glossary

This Appendix contains the glossary associated with this report.

Term	Definition
3GPP	The 3rd Generation Partnership Project (3GPP) is a collaboration agreement that was established in December 1998. The collaboration agreement brings together a number of telecommunications standards bodies which are known as "Organizational Partners".
Access Provider	An access provider is any organization that arranges for an individual or an organization to have access to the Internet.
Alliance for Telecommunications Industry Solutions (ATIS)	A U.S.-based organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. http://www.atis.org/
Department of Homeland Security (DHS)	Department of the Federal Government with five homeland security missions. These missions include preventing terrorism and enhancing security, securing and managing U.S. borders, enforcing and administering U.S. immigration laws, safeguarding and securing cyberspace, and ensuring resilience to disasters.
Geocoding	Translation of one form of location into another, typically a civic address into an x, y coordinate.
Geo Location	Latitude, longitude, elevation, and the datum which identifies the coordinate system used.
Geographic Targeting (geo-targeting)	The 47 CFR Part 10, Subpart D - Alert Message Requirements defines geographic targeting (geo-targeting) as follows: **"§ 10.450 Geographic targeting.** This section establishes minimum requirements for the geographic targeting of Alert Messages. A Participating CMS Provider will determine which of its network facilities, elements, and locations will be used to geographically target Alert Messages. A Participating CMS Provider must transmit any Alert Message that is specified by a geocode, circle, or polygon to an area not larger than the provider's approximation of coverage for the Counties or County Equivalents with which that geocode, circle, or polygon intersects. If, however, the propagation area of a provider's transmission site exceeds a single County or County Equivalent, a Participating CMS Provider may transmit an Alert Message to an area not exceeding the propagation area."
Geospatial	Data accurately referenced to a precise location on the earth's surface.
Global Positioning System (GPS)	A satellite based Location Determination Technology (LDT).
Spatial	Relating to, occupying, or having the character of space. Geographic Information Systems store spatial data in regional databases. See Geospatial.
Wireless Industry	Mobile Network operators and their equipment vendors (including device OEMs and OS implementers) who plan, standardize, develop, implement and maintain the commercial cellular mobile networks and devices.

Term	Definition
Working Group (WG)	A group of people formed to discuss and develop a response to a particular issue. The response may result in a Standard, an Information Document, Technical Requirements Document or Liaison.
X,y	Shorthand expression for coordinates that identify a specific location in two dimensions representing latitude and longitude.