ATIS-0700026

FEASIBILITY STUDY FOR WEA SUPPLEMENTAL TEXT

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

ATIS-0700026, *Feasibility Study for WEA Supplemental Text*

Is an American National Standard developed by the **Systems and Networks (SN)** Subcommittee under the **ATIS Wireless Technologies and Systems Committee (WTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0700026

ATIS Standard on

Feasibility Study for WEA Supplemental Text

Alliance for Telecommunications Industry Solutions

Approved December 2, 2015

Abstract

This feasibility study performs a technical analysis on supplemental information for Wireless Emergency Alert (WEA) Messages. This feasibility study is in response to Recommendations 5.1 and 5.2 of the December 2014 Federal Communications Commission (FCC) Communications Security, Reliability & Interoperability Council (CSRIC) Working Group 2 Wireless Emergency Alerts final report of December 3, 2014.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Wireless Technologies and Systems Committee (WTSC) develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies. WTSC develops and recommends positions on related subjects under consideration in other North American, regional, and international standards bodies.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, WTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, WTSC, which was responsible for its development, had the following leadership:

M. Younge, WTSC Chair (T-Mobile)

D. Zelmer, WTSC Vice-Chair (AT&T)

P. Musgrove, WTSC SN Chair (AT&T)

G. Schumacher, WTSC SN Vice-Chair (Sprint)

D. Sennett, Technical Editor (AT&T)

The Systems and Networks (SN) Subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

ATIS Standard on –

Feasibility Study for WEA Supplemental Text

1 Scope, Purpose, & Application

1.1 Scope

The scope of this document is a feasibility study of supplemental information for Wireless Emergency Alert (WEA) Messages based on recommendations from the Federal Communications Commission (FCC) Communications Security, Reliability & Interoperability Council (CSRIC).

1.2 Purpose

At the December 3, 2014 meeting, the FCC CSRIC approved the final report from the CSRIC Working Group 2, Wireless Emergency Alerts [Ref 1].

The FCC has received the recommendations from the CSRIC working group and, at the time of the completion of this feasibility study, the FCC has issued a Notice of Proposed Rulemaking (NPRM). The CSRIC working group report does contain recommendations that require action by the Alliance for Telecommunications Industry Solutions (ATIS). Specifically, Recommendation 5.1 [Ref 1] (as quoted below) tasks industry to study supplemental text for WEA alerts:

> *"**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 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 of the CSRIC working group report [Ref 1] (as quoted below) requires the study be completed one year after acceptance of the recommendation by the CSRIC (which was accepted on December 3, 2014).

"***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."*

1.3 Application

This feasibility study is applicable to cellular network operators, to the FCC, to the FCC CSRIC, and to the members of the regular WEA partner meetings which include the FCC, the Cellular Telecommunications Industry Association (CTIA), the Department of Homeland Security (DHS), the Federal Emergency Management Agency (FEMA), the National Weather Service (NWS), and cellular network operators.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 1] FCC CSRIC IV Working Group 2, *Geographic Targeting, Message Content and Character Limitation Subgroup Report*, October 2014.[1]

[Ref 2] ATIS-0700023, *ATIS Feasibility Study for LTE WEA Message Length*, October 2015.[2]

[Ref 3] 3GPP TS 22.146, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Stage 1*.[3]

---

[1] Available from the FCC at:

< http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_CMAS_Geo-Target_Msg_Content_Msg_Len_Rpt_Final.pdf >.

[2] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < https://www.atis.org/docstore/product.aspx?id=28243 >.

[3] This document is available from the 3rd Generation Partnership Project (3GPP) at: < http://www.3gpp.org/ >.

[Ref 4] 3GPP TS 23.246, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description*.[3]

[Ref 5] Abhinav Jauhri, Martin Griss & Hakan Erdogmus, Carnegie Mellon University, *Small Polygon Compression for Integer Coordinates*; presented June 12, 2015 at American Meteorological Society 43rd Conference on Broadcast Meteorology / 3rd Conference on Weather Warnings and Communication.[4]

[Ref 6] Michele Wood, Hamilton Bean, Brooke Liu & Marcus Boyd, DHS START, *Comprehensive Testing of Imminent Threat Public Messages for Mobile Devices: Updated Findings*; August 2015.[5]

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

3.1 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
API	Application Programming Interface
ATIS	Alliance for Telecommunications Industry Solutions
CB	Cell Broadcast
CBC	Cell Broadcast Center
CBE	Cell Broadcast Entity
CFR	Code of Federal Regulations
CMAS	Commercial Mobile Alert System
CMSP	Commercial Mobile Service Provider
CSRIC	Communications Security, Reliability & Interoperability Council
CTIA	Cellular Telecommunications Industry Association
DHS	Department of Homeland Security
eMBMS	Enhanced Multimedia Broadcast Multicast
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
HCI	Human-Computer Interaction

[4] Available at: < https://ams.confex.com/ams/43BC3WxWarn/webprogram/Paper273645.html >. (Last visited October 21st 2015).

[5] Report available from DHS at:

< http://www.firstresponder.gov/TechnologyDocuments/WEA%20-%20Comprehensive%20Testing%20of%20Imminent%20Threat%20Public%20Messages%20for%20Mobile%20Devices%20Updated%20Findings.pdf >. (Last visited October 21st 2015).

IPAWS	Integrated Public Alert and Warning System
ITU	International Telecommunications Union
JPEG	Joint Photographic Experts Group
NPRM	Notice of Proposed Rulemaking
NWS	National Weather Service
OS	Operating System
RAT	Radio Access Technology
SAME	Specific Area Message Encoding
URL	Uniform Resource Locator
UXD	User Experience Design
WEA	Wireless Emergency Alerts
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

4 Assumptions

This clause provides some of the assumptions made within this feasibility study.

1. The supplemental WEA messages will be applicable only for LTE.
2. The maximum size of the displayable text of a current WEA message per the standard is 90 GSM 7 bit displayable characters. The feasibility study for LTE Message Length Analysis [Ref 2] has studied the feasibility to extend this value to 360 GSM 7 bit displayable characters. This study is based upon the possible extended length of 360 displayable characters.

5 Considerations Based Upon Existing WEA Structure

This clause describes various considerations for supplemental information based upon the existing WEA structure and based upon the assumptions in clause 4. These topics are described in the following sub-clauses of this feasibility study:

- Considerations for display of WEA alert maps.
- Considerations for displaying photos for Amber Alerts.
- Considerations for displaying hazard alert symbols.
- Considerations for association of WEA Alert Message with CAP alert message.
- Considerations for embedded URLs.

5.1 Considerations for Display of WEA Alert Maps

Currently geocodes (i.e., Specific Area Message Encoding (SAME)/ Federal Information Processing Standards (FIPS), polygon, or circle coordinates) are used by the Cell Broadcast Entity/Cell Broadcast Center (CBE/CBC) exclusively to determine which cell sites should broadcast a WEA Alert Message. The geocoded are not

transmitted to the mobile device. Sending the geocodes to the mobile device is a fundamental change in the way WEA operates today, and will require years of standardization, product development, and deployment.

With that in mind, if a geocode that depicts the actual alert area is available in the mobile device, it may be possible to display it to the user. Furthermore, if the mobile device's location is known, it can optionally be included in the display of the alert area. Figure 5.1 shows how this might look like.

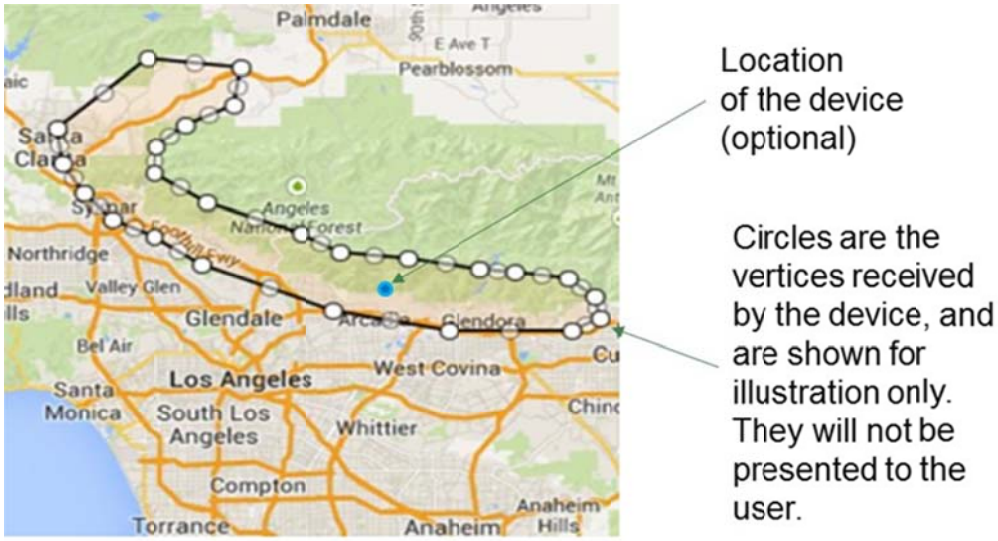

Figure 5.1 – Example Map Display with Polygon of Alert Area

There are a number of major issues to be addressed in order to enable such a feature:

1. The WEA app currently resides in the mobile device's OS (e.g., Android, iOS, Windows, BlackBerry, etc.). If 3rd party downloadable apps are to be allowed access to the received vertices, then Application Programming Interfaces (APIs) should be specified in order to enable the transfer of relevant information (e.g., polygon vertices) to the 3rd party app. See clause 8 for considerations related to APIs.
2. There is a limit on the number of octets that can be broadcasted to the mobile device. Polygons can have many vertices that will require truncation and/or compression to fit a WEA broadcast message packet size.
    a. Carnegie Mellon University has developed a report on a possible compression technique for polygon coordinates [Ref 5]. However, the wireless industry will need to review the technique for applicability in mobile devices, and industry standards would need to be developed to support a globally standardized compression technique.
3. A consumer behavior study must be conducted to determine how detailed the map and geocodes should be displayed.
    a. The following statements related to maps are contained in the Conclusions and Future Research of the DHS S&T research paper "Comprehensive Testing of Imminent Threat Public Messages for Mobile Devices: Updated Findings" [Ref 6]:
        - "None of the map elements tested had a statistically significant effect on message outcomes, and focus group participants varied widely in their reactions to the tested maps. Maps can be useful in message personalization, but the role they play varies based on message length."
        - "Adding maps to shorter 90 and 140-character messages seemed to help increase message understanding, but adding maps to longer messages decreased message understanding."

            NOTE: the conclusion of the ATIS feasibility study on LTE WEA message length [Ref 2] is 360 displayable characters.

        - "Consequently, maps should not be used in WEA messages without further research

examining the best way to craft such maps, as well as how they may impact message personalization and other outcomes."

- "Specifically, additional research is needed to determine how to best communicate hazard and receiver location in maps associated with WEA messages. Future research also should examine the extent to which humans are able to process text and visual information in an emergency context."

4. If the mobile device does not have mapping data (map) of the alert area, it will need to download it. A large number of mobile devices attempting to download maps simultaneously in a given area will have a negative impact on the operation of the cellular network in that area. This could happen at a time when network operation is critical and the capability for the subscriber to call 911 could be impeded. Some alternatives to mitigate this issue are:
    a. Include a high-level map in the mobile device app. This will increase the size of the app. Also, should the map cover a city, State, the U.S., or the whole world for the roamers? What should be the resolution of such a map? What kind of map is displayed (civic features vs. geographic features)?
    b. Enable map downloads in the background when the mobile device has a Wireless Fidelity (Wi-Fi) connection, which will require the mobile device to have Wi-Fi capability. Also, it does not address the case when a map is needed but there is no Wi-Fi connection accessible to the user in the area.
    c. The maps are downloaded in advance of being needed during non-busy hours based upon the serving location of the mobile device. This option could be subject to the carrier's policy.
5. Issues of charging, data subscriptions, and mobile device location.
6. For a mobile device to optionally display its location on the map, the user must enable the location services on the mobile device. This will have privacy issues and will also impact the mobile device's battery life. This option will not be available if the location service is not enabled. This may also have impact on the Commercial Mobile Service Provider (CMSP) network. Furthermore, location may not be available at the time of display.
7. The high level user interface design (UXD) or information flow needs further definition to address such issues as:
    a. If the mobile device receives text alerts as well as geocodes, how would it present them to the users in such a way that will help the user to take the appropriate action instead of potentially causing more confusion?
    b. Should both WEA text and map be presented?
    c. Should the mobile device wait for the WEA map to become available before displaying the WEA text?
    d. Will the user have to take an action to display WEA alert map?
    e. Should there be a message association between WEA text and its corresponding WEA map?
    f. What if the WEA map is associated with Presidential-level WEA text?
8. Backward compatibility must be addressed as only new mobile devices will be able to display WEA alert maps.
9. How will displaying a map help users to take the appropriate course of action in an emergency? This will require a behavioral study as well as public education.

In summary, there are a number of technical and behavioral issues that must be addressed before WEA alert maps are made available to the users. It will take time to specify the APIs to broadcast geocodes and text alerts concurrently. Furthermore, it will take even more time to upgrade the network and build new mobile devices capable of displaying WEA alert maps.

5.2 Considerations for Displaying Photos for Amber Alerts

Delivering photos to the mobile device and subsequent presentation to the user as part of WEA messages is being proposed primarily in conjunction with Amber Alerts. The typical desired scenario is that in an Amber Alert WEA message the following contents are included: a name and photo of the missing person is distributed; the date and location the person was last seen; and a contact number to use to report any information relating to the missing person.

Here the issue of possibly distributing and presenting a photo associated with an Amber Alert is discussed.

5.2.1 Amber Alert Photo Presentation

Current image compression techniques such as those defined by the Joint Photographic Experts Group (JPEG) aim at efficient and scalable compression of digital images with minimal reduction of image quality. These tools have such widespread use in digital cameras and web applications as to be considered ubiquitous. However, even with the application of these tools, the compressed Amber Alert images would still be impractical to be broadcast through current WEA cell broadcast capabilities as detailed in the next clause. It is assumed that only generally available and used compression tools already accessible in most smartphones would be used rather than creating a specialized and limited use capability optimized specifically for WEA cell broadcast.

5.2.2 Amber Alert Photo Transfer to Mobile Device

There are two ways that an Amber Alert photo could be transferred to a mobile device for presentation to the user. One way is a push mechanism where the photo is broadcast to all mobile devices in the designated area. The other way is a pull mechanism where a link (URL) is broadcast to all mobile devices in the designated area and each mobile device retrieves the image file individually.

5.2.2.1 Push Broadcasting Image Files through WEA Messages

The primary limitation for push broadcasting of Amber Alert photo content in WEA messages is one of requiring a large number of WEA messages to convey even a relatively small photo to the mobile device. WEA messages have a proposed limit of 360 characters for each message, and a thumbnail photo of about 1.5"x1.5" with a resolution of 72 dots per inch (DPI) will produce an image of 120x120 pixels. If 8 bit color scale is used, then a digital image file will be about 14,400 bytes in size. If we assume a 25% compression, then the resulting image file to broadcast would be 3600 octets. If a WEA message for broadcasting binary content were to be defined, the example described above would require at least 11 WEA binary messages to broadcast a small image file at the proposed WEA maximum of 360 characters.

For a more typical example, current point and shoot digital cameras range from 2 to 29 Megapixels with most ranging from 7 to 24 Megapixels. If we assume a typical camera at the low end of the majority of the cameras at 7 Megapixels, a typical photo size of 3072x2304 pixels at 72 DPI and 24 bit color scale might compress down to 2% of the raw image file size. The resulting file would still be around 3,000,000 octets and would require at least 9,000 of these additional WEA binary messages to broadcast a typical low end digital photo. This would take over 48 hours for each image broadcast using current WEA cell broadcast capabilities.

Note that these examples given are only a rough approximation of image size, resolution, color scale, and compression factors. In particular the compression factor is affected by image details of the file being compressed.

Additional complexity and overhead would be required to segment the digital image file by the message originator and reassemble it in the mobile device, further increasing the number of WEA messages required to broadcast a digital image file. Further mobile device functionality and complexity would be required to handle error recovery conditions such as if the mobile device would receive duplicate image file segments or is missing portions of the image file.

5.2.2.2 Pull Transfer through Broadcasting a URL

The pull approach of just delivering a link to a photo (URL to a digital image file) to display is a specific case of the more general topic of broadcasting URLs in WEA messages and is covered in clause 5.5 of this document.

5.2.3 Presentation of Amber Alert Photo and Text Together

The WEA Amber Alert text message with information about the missing person should be displayed together with the photo if that photo is broadcast in a separate WEA messages.

Work would be needed to specify the handling of digital images on the mobile device. The mobile device would need to know how to recognize that a portion of the image file is contained in a WEA message and it would have to link it with the associated WEA text message for concurrent presentation.

A mobile device that does not support receiving and displaying Amber Alert digital images should ignore the WEA messages containing portions of the digital images. Various error condition handling may need to be established such as when a WEA Amber Alert text message is received but the corresponding photo is not received.

5.3 Considerations for Displaying Hazard Alert Symbols

One of the enhancements to WEA proposed for study in the CSRIC IV Working Group 2 Report [Ref 1] is the capability to display hazard symbols (to be defined) that pictographically represent the type of warning being conveyed (e.g., fire, tornado, flood, chemical spill, etc.) to reinforce the significance of the public emergency situation described in the text portion of a WEA alert. The CSRIC IV Working Group 2 Report [Ref 1] noted that the hazard symbols used in WEA alerts are to be defined. A standard set of hazard symbols must be defined as no standard hazard symbols exist for alerts issued by the NWS, for example. In order to ensure that the use of hazard symbols improves the usability and accessibility of the individual alert, a User Experience Design (UXD) covering the Human-Computer Interaction (HCI) for the mobile user should be undertaken by the WEA stakeholders. To ensure the symbols are internationally recognized, such a UXD will require global participation, with standardization in the International Telecommunications Union (ITU) or other recognized fora.

The UXD would answer such questions as:

- What is the standard internationally-recognized hazard symbol set to be used with WEA?
- When is the hazard symbol presented to the user?
- How will the hazard symbols be presented for different disability accessibility modes, including use of colors?
- Will a WEA text alert always have an associated hazard symbol?
- How many hazard symbols could be presented to the user including multiple alerts?
- Is the hazard symbol always the same for a specific WEA warning type (such as alert category)?

This high level UXD would be used to develop the requirements for the hazard symbols and their use.

Since the use of hazard symbols in association with WEA alerts must support international roamers and is recommended to be adopted by other public warning systems in other countries, the hazard symbols themselves must have common, internationally agreed definitions (graphic icon, represented hazard, and encoding).

Once the UXD for the use of warning symbols has been developed along with the resulting requirements, the potential solutions can be investigated and the leading solution(s) selected for standardization by ATIS (initially) and other global standards bodies (e.g., 3GPP, ITU).

The solutions will need to support the following capabilities:

- Hazard warning icon delivery to the mobile device – potential solutions include:
  - Include the hazard symbol icons in the installed WEA client software image; or
  - Broadcast the hazard symbol icon each time it is referenced (this has the same considerations as an Amber Alert photo – see clause 5.2).
- Identification of which hazard symbol to present – potential solutions include:

- Have a new WEA message defined to specify the hazard symbol.
- Define a special character to indicate a hazard symbol to display (for example, the bio-hazard symbol has the Unicode encoding of U+2623).

5.4 Considerations for Association of WEA Alert Message with CAP Alert Message

In this clause, consideration for association of more than one WEA message is discussed. The use case is when the mobile device receives more than one copy of the same WEA message. This can happen in the following scenarios:

- The messages arrive through different Radio Access Technologies (RATs). An example of this scenario is when a mobile device receives alerts through CMSP, Satellite, and Wi-Fi concurrently.
- The messages arrive from different core networks. An example of this scenario is RAN Sharing where two carriers have different core networks but share eNodeBs.
- The mobile device changes RATs under the same carrier.
- The mobile device roams from one carrier to another carrier.

Per 47 Code of Federal Regulations (CFR) § 10.500 (g)[6], mobile devices are required to perform "Detection and suppression of presentation of duplicate alerts." So, presenting the same WEA message more than once violates this requirement.

Currently, duplication is detected in the mobile device using a combination of message ID and serial number. Serial numbers are unique only within a specific CMSP. The messages received from different CMSPs will be presented to the user more than once.

CMAC_message_number is unique across all CMSPs, but it is not sent to the mobile device.

Example: <CMAC_message_number>00001056</CMAC_message_number>.

So, one possible approach is to include the CMAC_message_number in the WEA message body that is sent to the mobile device. In such a scenario, the mobile device has to look inside the body of the message to detect duplication. This change applies only to Enhanced WEA on LTE (i.e., message length greater than 90 characters).

There are a number of issues to be addressed in order to enable such a feature:

1. This change could impact all the elements in the WEA path.
2. Backward compatibility should be investigated, as only new mobile devices may be able to understand CMAC_message_number in the body of WEA message.
3. The WEA message content must somehow be delineated so that it is not presented to the user.
4. The CMAC_message_number will reduce the number of displayable characters that can be presented to the user.
5. Need to investigate the situation of a mixed environment of legacy and enhanced WEA capabilities that will occur during the transitional phase at a minimum.

[6] Available from US Government Publishing Office at:
< http://www.gpo.gov/fdsys/granule/CFR-2009-title47-vol1/CFR-2009-title47-vol1-sec10-500 >.

5.5 Considerations for Embedded URL

One of the enhancements to WEA considered in the CSRIC IV Report [Ref 1] is to include URLs in WEA text alerts to allow the user to access richer (multi-) media with more complete and informative information about the emergency situation than is possible with just WEA text messages alone.

This clause examines the considerations to this approach, determines the usefulness, impact, cost, and complexity of any potential solution.

The basic flow for this discussion is assumed to be as follows:

1. The Alert Originator includes a URL pointing to the additional information for targeted users along with the basic alert text content.
2. The WEA Alert Message is broadcast to users in the designated area.
3. The smartphones that receive the text message would provide the user, upon viewing the basic alert text content, the option to request the additional information stored on a web server pointed to by the URL.
4. The user requesting the information ("clicking on a link") initiates a web (HTTP) request for the information over the Internet using typical web protocols.
5. The web server delivers the content to the mobile device that will then present it to the user using typical web clients.

The use of URLs in the WEA text message creates a hybrid approach between the current WEA text message broadcast and data transfers for each individual mobile device in the alert area. The benefits of the broadcast approach has already been considered when Cell Broadcast was compared to SMS (text messages) for distribution of WEA text alerts. The Cell Broadcast method was selected for its efficiency for reaching all mobile devices in a particular area in a relatively short period of time.

The difference in the use of URLs is that the mobile device, when it received a WEA text alert message with a URL would, when initiated by the user, request the alert content pointed to by the URL. So this saves the CMSP network from having to track and identify all mobile devices to send the content to as SMS does.

However there are still significant challenges to support using URLs in the WEA text messages. Plus, there are a few impacts on the WEA text message itself that would need to be addressed.

The use of URLs or Internet access can currently be done through three basic wireless paths:

1. Access the Internet through the CMSP's licensed spectrum (e.g., LTE) using a data subscription.
2. Access the Internet through CMSP's Wi-Fi offloading capability where the Internet traffic is transported over Wi-Fi instead of licensed spectrum to the CMSP's network and then sent on to its Internet destination.
3. Direct connection where the mobile device connects to the Internet directly through the Wi-Fi access bypassing CMSP management and control. The mobile device appears and acts like any other Wi-Fi device such as laptops and tablets.

For typical user access to web sites through the Internet, the web browser (client) will request Internet access without knowing or specifying which of the three Internet access methods are to be used. The mobile device will have a set of routing policies defined (by the vendor and/or CMSP) that establishes the priority of the three Internet access options to use. While the policies vary by mobile device, they generally all will consider the use of all available Internet access options. The result is that even if a direct Internet connection through Wi-Fi is the highest priority, if it isn't available (not connected to a Wi-Fi hotspot), the mobile device will then automatically use the CMSP's LTE Internet access. Mobile devices generally do not have Wi-Fi only routing policies.

A policy in the mobile device where URLs associated with a WEA text alert only use the direct Internet connection and not Internet connections through the CMSP network would have to be established in every smartphone.

The ability for a mobile device to use Wi-Fi instead of a CMSP's LTE Internet access is affected by a number of factors with the most important being:

- The Wi-Fi cannot be activated in the mobile device;

- There are no Wi-Fi networks accessible by the user (either not in range, or the user is not able to login to the Wi-Fi access point).

Therefore, not all users who receive a URL in a WEA text message on their smartphone will be able to use the direct Internet connection.

If the decision is made to use LTE for Internet access when direct Internet access is not available, impacts on the CMSP network would need to be investigated. When direct Internet access is available, the impact on the server providing the content that is referred to by the URL would need to be investigated.

This work should be based on additional studies on the typical distribution of mobile devices with and without direct Internet access during various key times of day (such as evening, commute times, work days, night time) as well as in different representative civic morphologies such as dense urban, urban, suburban, and rural settings.

The results of these studies would lead to modeling parameters to identify the potential traffic load on the CMSP network elements during an overload condition stemming from significant simultaneous access of WEA alert information web servers.

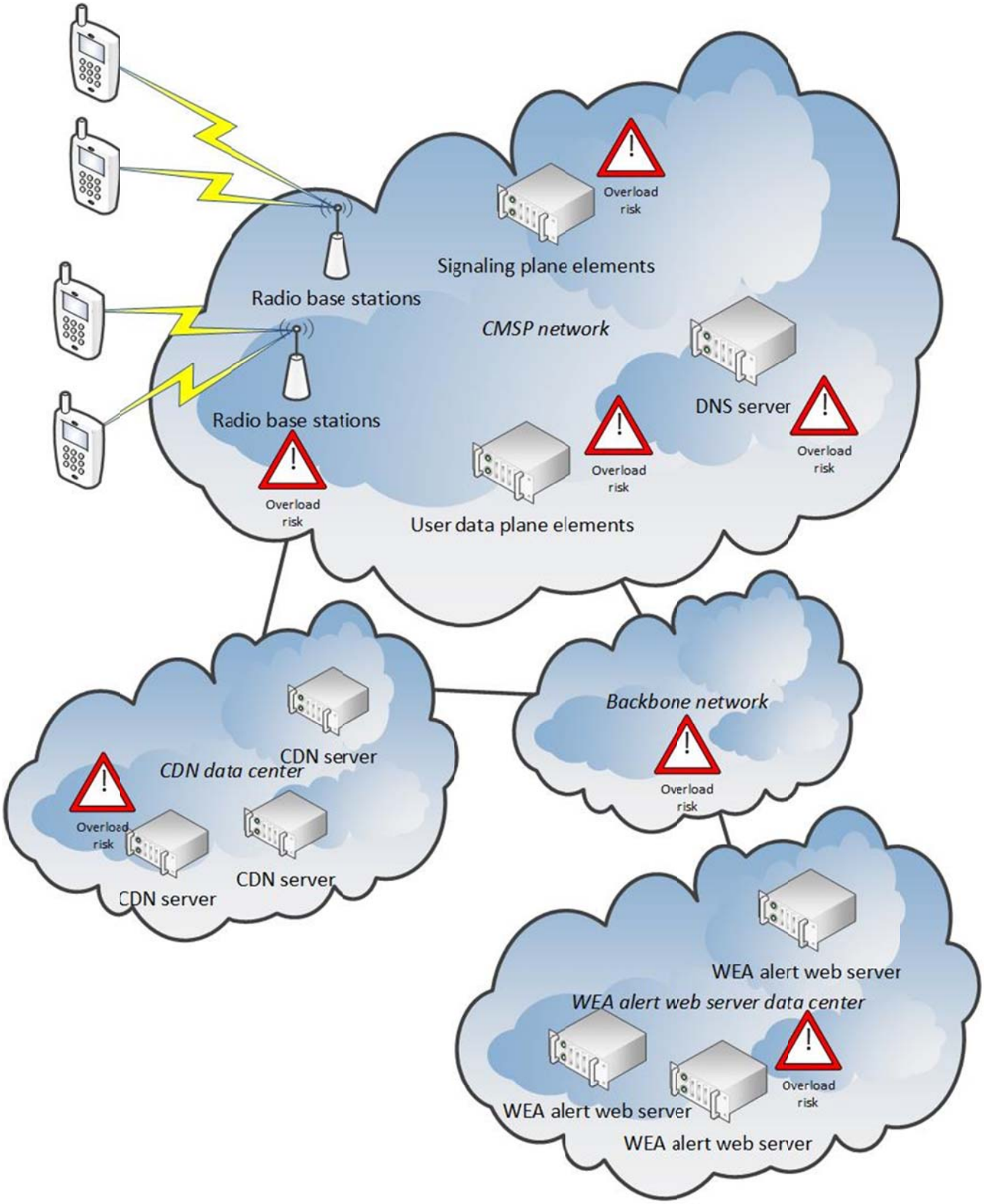

Figure 5.2 – Overload Risks of URL Use in WEA Text Alerts

Figure 5.2 illustrates some of the major network elements that would be used to deliver WEA alert content in response to the use of URLs in a WEA text alert. Sources (not exhaustive) of potential overload of these network elements are highlighted below:

- Radio base stations along with the cell sectors are dimensioned based on normal user behavior distribution where a certain portion of the users will be on active data sessions and others will be idle with minimal radio resources allocated. If a larger than usual number of users with idle mobile devices request the additional information indicated by the URL, the base station may be overloaded beyond its capacity for active data sessions.
- This surge in re-establishing active data sessions by idle mobile devices can also impact the signaling plane elements and the user data plane element from abnormal increase in signaling traffic and resources needed to handle data sessions.
- Another potential impact is that the additional simultaneous delivery of the additional alert content to users could exceed the capacity of one or more data links, leading to long delays in the user receiving the additional alert information, abandoning the effort, or retrying the request (leading to additional traffic). This can affect any point in the delivery of the content including the web server providing the information, the content delivery network (CDN) caching of the information, the backbone network or the CMSP user data delivery network elements.
- The DNS server translates the URL into an IP address used to route the URL request to the WEA alert web server. This critical step at the beginning of any web page retrieval means that the DNS server could also be overloaded with a flood of DNS requests related to near simultaneous WEA alert URL usage. The use of abbreviated URLs can also put additional traffic load on the DNS server since the abbreviated URL obtains the full length URL from the DNS server and then an additional DNS query returns the IP address for full length URL.
- While it may seem that a logical conclusion is that any bottlenecks in the alert information delivery network element such as WEA web servers will not impact the CMSP network transporting the content, it is highly probable that a significant number of user URL requests will be abandoned, either manually or automatically due to slow or no response from the WEA web servers, and re-attempted. This will result in additional DNS requests and content retrieval requests on already overloaded network elements including those in the CMSP network.
- There will also be data service subscription and charging implications for LTE access of WEA additional content retrieved from WEA web servers. The use of a URL to access WEA additional content assumes that it is done through the user's existing data subscription. There can be any number of business reasons why the user is unable to use their data service at the time of a WEA alert including – zero or low balance on a pre-paid account, account restricted due to non-payment of past charges, parental restrictions on children's Internet access, etc. Additionally, the data usage to retrieve the WEA additional alert information by URL will be charged against the user's data service account.

5.5.1 Cyber Security Mitigation

The assumption regarding URL usage as part of a WEA text alert message is that it would use existing web tools to deliver and present additional information supplementing the WEA text message including HTML, HTTP, JavaScript, and CSS. The issue of cybersecurity for the access of this web content will need to be addressed and appropriate mitigation approaches produced. It is expected that all aspects of cybersecurity would be evaluated including:

- DOS/DDOS attacks (DNS, webservers, etc.)
- DNS cache poisoning
- DNS spoofing
- Injection attacks
- Cross-site scripting
- Web server compromise

- Mobile malware distribution (Trojans, ransomware, bots, APTs, etc.)
- Insecure direct object references

In addition to documenting the cyber threat and risk assessment, mitigation approaches and the responsible organization is expected to be covered. Some of the cybersecurity mitigations are beyond the scope of CMSP WEA responsibility. The FCC and/or Congress need to address any additional CMSP liability aspects.

5.5.2 Subscriber Charges and Internet Access Restrictions for Retrieving Additional WEA Alert Information through WEA Text Alert URLs

Retrieving additional WEA alert information via a URL included in the WEA text message, if done without special action by the CMSP, would be through the user's Internet packet data service. The user would therefore need a packet data service subscription not restricted such as due to lack of funds (pre-paid) or delinquent payments (post-paid). The CMSP may have other data service restrictions such as parental Internet access controls.

The user may need to have a separate subscription to the Wi-Fi network selected by the mobile device.

Exceptions to this approach such as not charging the user for WEA related URL data usage, allowing restricted data subscriptions to access WEA related additional content through a URL, or allowing uninitialized and unauthenticated mobile devices to access WEA related additional content[7] through a URL (e.g., a mobile device just purchased and not yet activated or without a Subscriber Identity Module (SIM)), add additional costs and complexities that require further study including the following:

- Identifying a WEA URL request.
- Distinguishing a WEA URL request from other URL requests.
- Identifying WEA additional content being delivered to the mobile device.
- Distinguishing WEA additional content from other web content being delivered to the mobile device.
- Restricting data service exceptions to only retrieve WEA additional content requested in a WEA text alert URL.
- Cybersecurity and fraud detection measures for any additional network elements and processing required to handle these exceptions.

The above items require significant development in the CMSP back office systems.

5.5.3 WEA Text Alert Message Impact from URL Usage

The primary impact of including a URL in a WEA text alert message is that it will use up part of the character limit available for WEA text message content. It will be up to the Alert Originators to ensure that the URL length can fit within a single WEA text message alert as well as allow sufficient space for the text message content.

If the URL is put into a WEA Alert Message separate from the text message content, then the challenge is to correlate the text content and URL WEA messages to each other for correct presentation to the user.

Likewise, backwards compatibility for mobile devices not expecting a URL as well as how feature phones will deal with a URL in the WEA text alert content.

To summarize the discussion, there are significant challenges to the use of URLs even if a direct Internet connection was readily available to practically all users at the time of an alert notification.

[7] Current FCC regulations do not require support of WEA alerting by uninitialized or unauthenticated mobile devices.

6 Considerations for Long Term Technologies

Most of the analysis in this feasibility study are based on using Cell Broadcast (CB) in LTE. There are a limited number of Octets that can be carried in a CB which, consequently, limits the amount of information that can be broadcasted. This is the reason why it is recommended that CB is used only to transmit text or small amounts of data.

Multimedia Broadcast Multicast Service in LTE (eMBMS), as specified in 3GPP TS 22.146 [Ref 3] and 3GPP TS 23.246 [Ref 4], is another technique to broadcast larger amounts of data (e.g., multimedia). The advantage of eMBMS is that it is a broadcast technology, similar to CB, which is more efficient than point to point communication. Also, unlike CB in LTE which uses SystemInformationBlock that is critical for the proper operation of an LTE system, eMBMS was designed to efficiently broadcast large amounts of user data.

There are, however, several issues with eMBMS for consideration to be used for WEA:

- eMBMS is not widely deployed as it is not required for the operation of an LTE system. Carrier deployment of eMBMS is based solely on the commercial business drivers and not voluntary support for WEA.
- There are standardization efforts to enhance eMBMS, but they are not considering WEA.
- eMBMS currently cannot be geo-targeted as well as CB in LTE. There are techniques being discussed to address this, but the standardization process is in its initial stages, and it is not considering WEA.
- Unlike CB, it is more challenging to broadcast an unscheduled program in eMBMS.
- Not all mobile devices will support eMBMS.
- Although eMBMS is more efficient than point to point techniques, it will require more system resources than CB.
- eMBMS will consume more power than CB in the mobile device, resulting in a negative impact to battery life.
- It is unlikely that eMBMS will ever be deployed as widely in networks and mobile devices as CB.
- There may be roaming issues that are not well-defined at present.

In summary, although eMBMS is an efficient technique to broadcast multimedia, it will take a few years to make technical changes to it so that it can support WEA efficiently.

7 Considerations for Usage of non-CMSP Networks

As defined by the WARN Act and FCC Part 10 rules, WEA obligations are on CMSPs that elect to participate. WEA messages are broadcast by participating CMSPs using capabilities in the cellular network infrastructure in accordance with FCC rules and industry standards. It is noted that many smartphone devices, in addition to supporting cellular technology also support Wi-Fi, and a much smaller subset can also support satellite communication. However, even mobile devices that have Wi-Fi capability may not have the Wi-Fi enabled by the user or be connected to a Wi-Fi network (e.g., no coverage or only secure networks available).

In this clause, consideration for support of an “emergency alerting” service over Wi-Fi and satellite are discussed. Note that the concept of detecting duplication in a mobile device that may receive WEA and potentially non-WEA alerts from multiple RATs was discussed in clause 5.4.

7.1 Considerations for Wi-Fi

At a high level, there are two categories of Wi-Fi connections. The first is interworking Wireless Local Area Network (WLAN), where CMSPs may use Wi-Fi for off-loading data traffic from the cellular network. Alternatively, the Wi-Fi network could be completely independent, and the CMSPs have no visibility or control over the data traffic that goes on the Wi-Fi connection.

If a mobile device is connected through both cellular and Wi-Fi, it will receive WEA through its cellular connection even while the user is using a Wi-Fi application (e.g., surfing the web).

If Wi-Fi calling is supported by the CMSP operator and the user is currently active in a Wi-Fi voice call, according to FCC rules there is no requirement to deliver the WEA message while an active call is in progress. The FCC rules are silent as to whether the call is active on the CMSP network or an alternate Wi-Fi network; in either case, WEA should not interrupt the voice call in progress.

If a mobile device is connected through a non-interworking Wi-Fi network, the Wi-Fi network operator has no obligation to provide emergency alerts, and the mobile device will not be able to receive WEA from CMSPs. Of course, it is possible that the mobile device may receive some form of non-WEA alert through 3rd party over-the-top apps. These non-WEA apps are outside the scope of CMSPs and this feasibility study.

Finally, if a mobile device is connected through an interworking WLAN only, it can still receive non-WEA alerts through 3rd party over-the-top apps. In addition, the capability for CMSPs to forward WEA to the mobile device when it is on the Wi-Fi connection will require much more technical analysis, standards work, and upgrade of cellular and Wi-Fi networks and mobile devices. Geo-targeting on Wi-Fi access presents significant technical challenges, which are beyond the scope of this study to detail.

7.2 Considerations for Satellite

Although satellite is not a CMSP service per FCC definition and thus does not follow the WARN Act or FCC Part 10 rules, it may be possible to broadcast some form of emergency alerts using satellite communication. The satellite footprint is much larger than a terrestrial cell/sector coverage area. So, geo-targeting a small area is practically impossible using satellite. Furthermore, since this is not WEA and CMSPs have no control over what is transmitted on satellite networks, it is not possible for CMSPs to enable WEA on satellite.

Note that many satellite networks already have a connection to the Integrated Public Alert and Warning System (IPAWS). How the Satellite Providers use the information provided to them is outside the scope of this feasibility study.

8 Considerations for Usage of Mobile Device WEA Data Accessibility by Trusted Developer Partners

This clause analyzes the feasibility of third party application support for WEA.

8.1 Mobile Device Trusted Developer Partner Access to WEA Alerts

Third party application access to WEA alerts on the mobile device may be provided by some mobile device platform vendors in the form of a published API and other mobile device platform vendors choose to keep the APIs private. CMSPs do not control or enforce what platform capabilities and behaviors are exposed to developers and what are hidden from developers.

Because of this, the CMSP's only potential role in a Trusted Developer Partner program is if distribution option 3 described in clause 8.2 is used, or a new distribution model is developed with the CMSP taking on the distributor role.

It is assumed that since at least one mobile device platform publishes the WEA alert access API and several applications are already available in the platform's Application Store, that it is the responsibility of the third party WEA alert application developer to deal with any of the following issues:

- Potential interaction with multiple WEA alert applications on the same mobile device (e.g., multiple alerting for the same broadcast WEA alert or different opt-out settings).
- Adhering to WEA regulations regarding presentation of WEA alerts such as distinctive tones and cadences as well as preventing any copying and forwarding of WEA alert content.
- Potential service interruptions through use of any Internet or cloud source of information or processing during any large scale WEA alerting scenarios where the packet data service is overloaded or

significantly delayed at any point in the network (described in the clause 5.5 discussion of URLs).

CMSPs are not in a position to evaluate or enforce any Trusted Developer Partner program requirements related to any third party WEA alert applications.

8.2 Third Party Application Distribution

Third party applications can be made available and distributed to a user's smartphone in at least the following different ways:

1. An application integrated into the core platform Operating System (OS) distribution by the platform vendor.
2. An application integrated into the OS distribution by the mobile device vendor.
3. An application built into a CMSP's specific mobile device OS platform.
4. An application available in the platform's Application Store that the user is able to find, download, and install in their smartphone.
5. An application available in an enterprise's Application Store when an enterprise provided mobile device is restricted to the enterprise Application Store.
6. An application downloaded from a web site or other Internet source.

A CMSP will typically specify that each mobile device certified to operate in the CMSP's network will have an application providing basic WEA alert detection and presentation capabilities available through distribution methods 1-3 described above.

For applications distributed by a platform's Application Store, the store operator sets the criteria for accepting applications offered by the store and provides the sole authorization of the store applications. The CMSP does not have any control over the applications offered by the platform's Application Store.

For applications distributed by an enterprise's Application Store, the enterprise sets the criteria for accepting applications offered by the store and provides the sole authorization of the store applications. The CMSP does not have any control over the applications offered by the enterprise Application Store. The enterprise Application Store will contain mostly a subset of the platform's Application Store offerings.

Applications downloaded from other sources such as web sites have no authorization at all. However, mobile device platforms usually explicitly require the user to opt-in to be able to install applications not offered in the platform's Application Store.

Any Trusted Developer Partner program will have to support these application distribution models, as well as identify how to address untrusted developers (e.g., enforcement).

9 Conclusions and Recommendations

9.1 Conclusions

This feasibility study provides a detailed study of the current WEA Supplemental Text. The analysis in this feasibility study is based, broadly, on using CB in LTE. The recommended extended WEA length is described in the ATIS Feasibility Study for LTE WEA Message Length [Ref 2]. Following are the conclusions of this study:

1. **Display of simple maps:** There are a number of technical and behavorial issues with displaying maps associated with WEA alerts. Some studies have shown adding maps to messages greater than 90-characters decreases message understanding. It will take significant time and development/deployment effort to enable the capability for a map display associated with a WEA Alert Message. Furthermore, it will take significant standardization, development time, and effort to upgrade the CMSP Infrastructure network and standardize and build new mobile devices capable of displaying maps associated with WEA alerts.

2. **Display of photos for Amber Alerts:** The issues surrounding the delivery of photographic images to the mobile device and presentation to the user as part of a WEA message is discussed in this feasibility study. Concepts such as photo broadcast, presentation, and transfer to the mobile device were studied. In addition, compression techniques for digital images were discussed. Although tools for compression of images exist, it is not practical to use such tools to broadcast images using existing cell broadcast capabilities, the technology used to broadcast text-based WEA Alert Messages. The text-based LTE broadcast technology is not designed to transmit large amount of data such as photos.

3. **Display of hazard symbols:** Another proposed enhancement evaluated in this WEA study is the definition and use of hazard symbols to pictographically represent the type of warning being conveyed. These symbols (e.g., fire, flood, chemical spill, etc.) would be designed to reinforce the significance of the public emergency that is represented in the text portion of the WEA alert. To ensure that the use of hazard symbols improve the usability and accessibility of an actual alert, a study of the UXD covering the HCI for the mobile user should be undertaken by the WEA stakeholders and would require global standardization. The hazard symbols would require a common, internationally agreed upon set of definitions, for example, graphic icon. The use of internationally recognized symbols will simplify public education efforts as well as reduce issues of language and cultural differences and understanding of the hazard symbols. It will also simplify most mobile devices which are developed for and deployed in worldwide markets.

4. **Embedded URL:** A number of considerations were given to the consequences of including an embedded URL in a WEA Alert Message, to determine the feasibility and impacts to the CMSP networks. The study concluded that introducing URLs in a WEA message will result in significant challenges within the CMSP infrastructure network. Network congestion to the point of blocking communications is a significant result of introducing URLs in a WEA Alert Message. In addition, the issue of cyber security for web access would need to be addressed appropriately. All aspects of cybersecurity should be evaluated as some of the cybersecurity mitigations are beyond the scope of CMSP WEA responsibility. The FCC and/or Congress need to address any additional CMSP liability aspects since the URL access is beyond the definition of CMSP obligation under the WARN Act. Subscriber charges and Internet access restrictions for retrieving additional WEA alert information through WEA text alert URLs would need to be considered or addressed in more detail.

5. **Long-term technologies:** A limited amount of information can be broadcasted using CB due to the limitation of the message length and for this reason it is recommended that CB be used only to transmit text. In LTE, a technique designed to broadcast large amounts of data (e.g., multimedia) is eMBMS. However, there are a number of challenges with eMBMS that should be considered in relation to WEA, e.g., eMBMS is not widely deployed and enhancements to eMBMS are being considered in the standards. However, these enhancements are not considering WEA requirements. It will take years to make technical changes to eMBMS standards to efficiently support WEA. eMBMS requires a significant upgrade to a CMSP network. CMSPs are not obligated to deploy eMBMS. CMSP deployment of eMBMS is based solely on the commercial business drivers and not voluntary support for WEA.

6. **Usage of alternative data networks:** Considerations for support of an “emergency alerting” service over Wi-Fi and satellite are also studied. Taking WEA into consideration, there are two categories for Wi-Fi connections: interworking WLAN and Wi-Fi independent connectivity. The capability for CMSPs to forward WEA messages to the mobile device when it is on a carrier-controlled interworking Wi-Fi connection will require much more technical analysis, standards work, and upgrade of CMSP network infrastructure, Wi-Fi networks, and mobile devices. WEA over independent Wi-Fi networks impose significant challenges since it is well beyond traditional CMSP-controlled WEA defined by the WARN Act. Geo-targeting on Wi-Fi access presents significant technical challenges, which are beyond the scope of this feasibility study. Regarding satellite, since the satellite footprint is much larger than cell/sector coverage, geo-targeting is much more difficult than in a CMSP network. In addition, since the satellite network is not a CMSP network, it is not feasible for CMSPs to enable WEA through satellite.

7. **Data accessibility by third party applications:** There are a number of elements for a Trusted Developer Partner program which will have to be established and are outside the scope of CMSP's control. One element is that the Trusted Developer Partner program will need to be aligned with the current distribution models for smartphone applications – Application Stores. Another element to cover is with only some smartphone platforms providing application (API) access to WEA alerts, the smartphone platforms without published WEA alert APIs will need to be approached to produce published WEA alert APIs. Any applications developed under the Trusted Developer Partner program that access Internet

based information or data will need to consider that the Internet access, either through CMSP LTE or Wi-Fi, may be compromised during a WEA alert broadcast which covers a wide or densely populated area. CMSPs are not in a position to evaluate or enforce any Trusted Developer Partner program requirements related to any third party WEA alert applications.

9.2 Recommendations

Based on the technical analysis of this feasibility study and considering all factors, ATIS recommends the following:

1. WEA Alert Messages should only contain textual content and should not include photos or maps since the cell broadcast technology does not support broadcast of the data needed to enable multimedia content.
2. The existing FCC rule specifying restriction on the inclusion of URLs in WEA Alert Messages should remain.
3. A study of the UXD covering the HCI including the display of hazard symbols for the mobile user should be undertaken by the WEA stakeholders followed by the associated global standardization.
4. CMSPs are not obligated to deploy eMBMS. Carrier deployment of eMBMS is based solely on the commercial business drivers and not voluntary support for WEA.
5. WEA is defined as a voluntary obligation on CMSPs and thus is not suitable for Wi-Fi or Satellite. Further detailed analysis is required regarding the support of an emergency alert service (non-WEA) via Wi-Fi or Satellite.
6. While third party applications may be used in conjunction with WEA, CMSPs are not in a position to evaluate or enforce any Trusted Developer Partner program requirements related to any third party WEA alert applications.

While this feasibility study does not conclude the need for modifications to existing WEA rules or standards, if through FCC action corresponding rule changes are made, implementation of those changes will require the cellular industry to undertake standards changes to ATIS and 3GPP standards, followed by modifications to the “C” interface between the FEMA IPAWS Federal Alert Gateway and the CMSP Gateway, and modifications to CMSP infrastructure and mobile devices. Related enhancements by the Alert Originator procedures and equipment will also be required for some of these items.