DRAFT

Commercial Mobile Alert Service Architecture and Requirements

DRAFT – September 24, 2007

Version	**0.6**
Revision Date	**9/24/2007**

Table of Contents

List of Figures

List of Tables

1 Introduction and Executive Summary

1.1 Executive Summary

On October 13, 2006, the President signed the Security and Accountability For Every Port (SAFE Port) Act1 into law. Title VI of the SAFE Port Act, the WARN Act, establishes a process for commercial mobile service providers (CMSPs) to voluntarily elect to transmit emergency alerts. Section 603 (c) of the WARN Act required that the Federal Communications Commission (Commission) establish the Commercial Mobile Service Alert Advisory Committee (CMSAAC) to develop and recommend technical standards and protocols for the voluntary transmission of emergency alerts by CMSPs within one year from the date of enactment of the WARN Act. (i.e., by October 12, 2007).2 This document presents the result of the CMSAAC's efforts to satisfy the obligations set forth in the WARN Act.

The WARN Act places the following tasks before the CMSAAC. Each is followed by the Section number or numbers in this report that includes recommendations addressing the associated WARN Act's requirements:

Within one year after the enactment of this Act, the Advisory Committee shall develop and submit to the Federal Communications Commission recommendations –

1) For protocols, technical capabilities, and technical procedures through which electing commercial mobile service providers receive, verify, and transmit alerts to subscribers (Sections 2, 4, 6, 8, 10);
2) For the establishment of technical standards for priority transmission of alerts by electing commercial mobile service providers to subscribers (Sections 2, 9);
3) For relevant technical standards for devices and equipment and technologies used by electing commercial mobile service providers to transmit emergency alerts to subscribers (Sections 7, 9;
4) For the technical capability to transmit emergency alerts by electing commercial mobile service providers to subscribers in languages in addition to English, to the extent practicable and feasible (Section 5);
5) Under which electing commercial mobile service providers may offer subscribers the capability of preventing the subscriber's device from receiving emergency alerts, or classes of such alerts, (other than an alert issued by the President), consistent with Section 602(b)(2)(E) of the WARN Act (Section 5);
6) For a process under which commercial mobile service providers can elect to transmit emergency alerts if
   a) not all of the devices or equipment used by such provider are capable of receiving such alerts (Section 3); or
   b) the provider cannot offer such alerts throughout the entirety of its service area (Section 3); and
7) As otherwise necessary to enable electing commercial mobile service providers to transmit emergency alerts to subscribers.

Following are summaries of each section in the document, with a focus on the recommendations the CMSAAC makes in each. This section is provided as a high-level overview only and is not intended as a substitute for the formal recommendations of the CMSAAC, which are laid forth in subsequent sections of the document, many of which are highly technical.

1.1.1 Reference Architecture (Section 2)

This section recommends a functional reference model for the distribution of alerts to Commercial Mobile Service Providers (CMSPs) (see Section 2.1). Under this reference model, a Federal government entity, the "Alert Aggregator," would receive, aggregate, and authenticate alerts originated by authorized alert

[1] CITE
[2] Section 603(c) of the WARN Act

initiators using the Common Alerting Protocol (CAP). The government entity would also act as an "Alert Gateway" (see Section 2.2) to formulate a 90 character alert based on key fields in the CAP alert sent by the alert initiator3. Based on CMSP profiles maintained in the Alert Gateway, the Alert Gateway would then deliver the alert over a secure interface (see Section 2.3.1) to another gateway maintained by the appropriate CMSP "CMSP Gateway." (see Section 2.3.2)

Each individual CMSP Gateway would be responsible for the management of the particular CMSP elections to provide alerts in whole or in part. The CMSP Gateway would also be responsible for formulating the alert in a manner consistent with the individual CMSP's available delivery technologies, mapping the alert to the associated set of cell sites / paging transceivers, and handling congestion within the CMSP Infrastructure. The CMSP Gateway will process alerts in a first in – first out (FIFO) queuing method except for a Presidential-level alert, which will be immediately moved to the top of the queue and processed before all other non-Presidential alerts.

Upon receipt of an alert from the CMSP Gateway, the CMSP Infrastructure distributes the received CMAS alert message to the determined set of cell sites/paging transceivers and authenticates interactions with the Mobile Device (see Section 2.3.3). Ultimately, the alert is received on a customer's Mobile Device. The major functions of the Mobile Device are to authenticate interactions with the CMSP Infrastructure, to monitor for CMAS alerts, to maintain customer options (such as the subscriber's opt-out selections and subscriber's preferred language, if applicable), and to activate the associated visual, audio, and mechanical (e.g., vibration) indicators that the subscriber has indicated as options when aln alert is received on the Mobile Device. (see Section 2.3.5.)

1.1.2 Deployment Scenarios (Section 3)

This section notes that the WARN Act specifies that a CMSP who elects to transmit emergency alerts can elect to transmit the CMAS alerts "in whole or in part."4 The CMSAAC defines "in whole or in part" as including all or a subset of the CMSP's service area, and/or all or a subset of current and future mobile devices supported by the CMSP network. The section then posits a set of scenarios in which an individual alert is sent over CMSP networks that deploy various technologies and handsets that may or may not support the transmission of the alert. (Sections 3.1-3.3). This section also contains recommendations for the notices to subscribers that the WARN Act requires where a CMSP does not elect to provide alerts. (see Section 3.4).

1.1.3 CMAS Alert Scenarios (Section 4)

This section provides descriptions of a representative sample of scenarios and message flows related to the transmission and support of CMAS Alerts. The section includes descriptions and charts of scenarios involving text based streaming audio or streaming video CMAS alert, CMAS alert cancellation, CMAS alert updates, CMAS alert expiration, duplicate CMAS alerts, and multiple different active CMAS alerts.

1.1.4 General Recommendations and Conclusions (Section 5)

This section sets forth the CMSAAC's recommendations concerning the extent and scope of CMAS alerts. The major recommendation in this section is that there be three classes of Commercial Mobile Alerts: Presidential-level, Imminent threat to life and property; and Child Abduction Emergency or "AMBER Alert"Service. (see Section 5.1). The section also recommends a format for CMAS alerts (se Section 5.3.1.) and a method for extracting a CMAS alert from CAP fields and free form text (see Section 5.3.2.). The section also recommends that alert initiators be trained on creating CMAS alerts (see Section 5.3.4).

A significant recommendation concerns the geo-targeting of CMAS alerts. The CMSAAC acknowledges that it is the goal of the CMAS for CMSPs to be able to deliver geo-targeted alerts to the areas specified by the alert initiator. However, early CMAS implementations will likely be limited to static geo-targeting areas. Hence, the CMSAAC recommends that, initially, geo-targeting be at least precise enough target at

[3] Provisions have also been made for authorized alert originators to formulate and distribute alerts via the Alert Gateway in free text.
[4] Section 602(c).

the county level. The CMSAAC further recognizes that certain areas with especially urgent alerting needs have a need for more precise geo-targeting, and provisions are made to accommodate them. Longer term the CMSAAC recommends that provisions in Section 604 of the WARN Act be applied to fully realize the benefits of dynamic geo-targeting. .

This section also makes recommendations on the needs of users, including individuals with disabilities and the elderly. Among the major recommendations in this is the requirement for the CMAS to support a common audio attention signal and a common vibrating cadence to be used solely for CMAS alerts. Further, the CMSAAC recommends that the alert initiator use clear and simple language whenever possible, with minimal use of abbreviations and that the mobile device provide an easy way to allow the user to recall the message for review. 5.5.3

The section notes that the WARN Act provides for subscriber CMAS alert Opt-Out, and recommended that CMSPs shall offer their subscribers a simple opt-out process that is based on the classification of imminent threat and AMBER Alerts. Except for presidential messages, which are always transmitted, the process should allow the choice to opt-out of (1) All messages, (2) All severe messages, or (3) AMBER Alerts. Regarding the transmission of CMAS alerts in languages other than English, the CMSAAC has analyzed the technical feasibility of supporting multi-language CMAS alerts on various delivery technologies and has determined that support of languages other than English is a very complex issue and that, at the present time, the CMSAAC believes there are fundamental technical problems to reliably implement any languages in addition to English.

Finally, the CMSAAC notes that roaming is only supported on an intra-technology basis.

1.1.5 Service Profiles (Section 6)

In this section the CMSAAC notes that the CMAS architecture and recommendations are based upon the principles of technology-neutral service profiles containing, for example, profiles for maximum payload and displayable message size. The section defines service profiles for: (a) Text; (b) Streaming Audio (future capability); (c) Streaming Video; and (c) Downloaded Multimedia Profile (future capability), and provides general recommendations and conclusions for each.

1.1.6 Mobile Device Functionality for CMAS Alerts (Section 7)

This section describes the impact to the mobile devices. i.e., the handsets, for the support of CMAS alerts. The section includes the recommend that if the end user has both muted the mobile device audio and alarms and/or has deselected or turned off the vibration capabilities of the mobile device, neither the CMAS audio attention signal nor the special emergency alert vibration cadence will be activated upon receipt of a CMAS alert. Further, the section recommends that, in order to minimize the possibility of network congestion and false alerts, mobile devices should not support any user interface capabilities to forward received CMAS alerts, to reply to received CMAS alerts, or to copy and paste CMAS alert contents. The section also notes that the monitoring for CMAS alerts could have a significant impact on handset battery life, but that with modifications to network infrastructure, mobile devices and/or standards, the reduction of battery life can be less than 10% of today's capability for monitoring.

1.1.7 Security for CMAS Alerts (Section 8)

This section recommends a specific Alert Aggregator and Alert Gateway Trust Model to assure the security, authentication and authorization of alerts from the Alert initiator to the CMAP Gateway. The section then recommends security requirements for the interface between the Alert and CMSP Gateways and within each CMSP's network.

1.2 CMAS Reliability & Performance (section 9)

Recommendations in this section include Alert Gateway performance requirements such as the capability to monitor system utilization for capacity planning purposes, and to temporarily disable and buffer CMAS alert traffic in the event of an overload. The CMSAAC acknowledges the importance of assessing any latency in alert delivery, but notes that it will be difficult to predict system performance in this area prior to deployment. The CMSAAC suggests that factors relevant to potential latency include; mobile device

battery life impact, call processing impact; capabilities of the delivery technology; message queues; number of languages; number of targeted cell sites/paging transceivers for the alert area; and any geo-targeting processing. Similarly, although the CMSAAC recommends that the CMAS end-to-end reliability technology meet telecom standards for highly reliable systems, the over-all reliability of CMAS is unpredictable because RF transmissions can be subject to noise and other interference or environmental factors; the capabilities of the cellular environment are not predictable especially in a disaster environment; the subscriber may be in a location that does not have any RF signal; and the subscriber's mobile device may not have any remaining power. In order to assure the reliability and performance of this new system, the CMSAAC recommends procedures for logging CMAS alerts at the Alert Gateway and for testing the system at the Alert Gateway and on and end-to-end basis.

1.2.1 Interface Protocols for CMAS Alerts (Section 10)

This section establishes detailed technical protocols and specifications for the delivery of alerts over the various interfaces in the Reference Model. Specifically, the section established requirements that Alert Initiators must meet to deliver CMAS alerts to the Alert Aggregator, and that the Alert Gateway must meet to delver CMAS alerts to the CMSP gateway. CAP mapping parameters are provided in detail.

1.3 Definitions

Commercial Mobile Alert (CMA) – The term CMA refers to the event that creates the need for a CMAM and can fall into any of the following three categories: i) a Presidential alert, ii) an imminent threat to life and property, or iii) an AMBER alert.

Commercial Mobile Alert Message (CMAM) – The term CMAM refers to communication that is issued to the end-user via the Commercial Mobile Alerting System in response to i) a Presidential alert, ii) an imminent threat to life and property, or iii) an AMBER alert.

Commercial Mobile Alert Service (CMAS) – The term CMAS refers to the end-to-end architecture for delivery emergency alert messages subject to the WARN Act.

Commercial Mobile Service Provider (CMSP) – Per the WARN Act Section 602 (b) (1) (A), a CMSP is a licensee providing commercial mobile service as defined in section 332 (d) (1) of the Communications Act of 1934 (47 U.S.C. 332 (d) (1)), where the term "commercial mobile service" means any mobile service that is provided for profit and makes interconnected service available

1.4 Acronyms

AMBER.....America's Missing: Broadcast Emergency Response

CAP.....Common Alerting Protocol as defined in CAP version 1.1 specification

CDMA.....Code Division Multiple Access

CMA.....Commercial Mobile Alert

CMAM.....Commercial Mobile Alert Message

CMAS.....Commercial Mobile Alert Service

CMSAAC.....Commercial Mobile Service Alert Advisory Group

CMSP.....Commercial Mobile Service Provider

CTIA.....Cellular Telecommunications Industry Association

EOC.....Emergency Operations Center

FIPS.....Federal Information Processing Standards

GSM.....Global System for Mobile communications

NOAA	National Oceanic and Atmospheric Administration
MVNO	Mobile Virtual Network Operator
NIST	National Institute of Standards and Technology
NWS	National Weather Service
SAME	Specific Area Message Encoding
SMS	Short Message Service
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
WARN	Warning, Alert, and Response Network
XML	Extensible Markup Language

2 Reference Architecture

2.1 Functional Reference Model Diagram

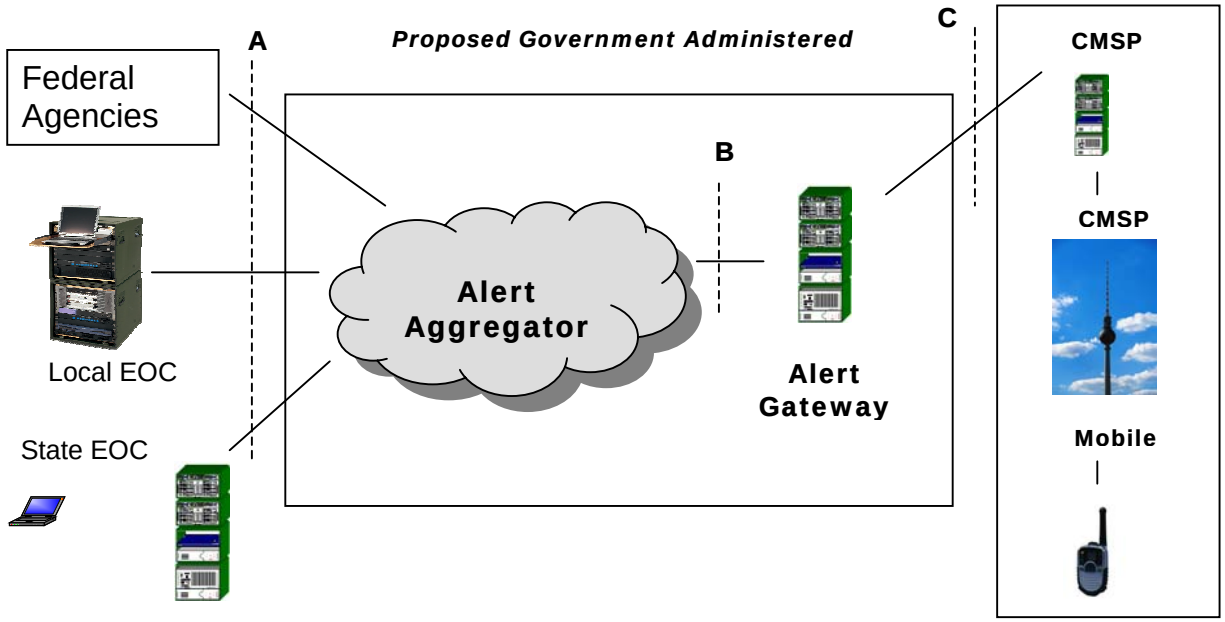

Figure 2-1 CMAS Functional Reference Model

2.2 Government Administered Elements Definitions & Requirements

The CMSAAC recommends that the Alert Aggregator and Alert Gateway be the responsibility of the authorized government entity. The CMSAAC further recommends that the system be acquired, managed, operated, and administered by the authorized government entity.

2.2.1 Reference Point A

The actions to be performed at Reference Point A include the following:

1. Provide information for the authentication and validation of actions across this reference point.
2. Delivery of a new, updated, or cancelled wireless alert message to Alert Distribution Network in CAP format.
3. Acknowledgement from Alert Gateway to Alert Aggregator that the new, updated, or cancelled wireless alert message has been received by the Alert Gateway.

2.2.2 Alert Aggregator

The CMSAAC recommends that the authorized government entity operate an alerting framework that aggregates all alerts submitted by Federal, State, Tribal and local originators and deliver these alerts to the

Alert Gateway. The CMSAAC makes the following additional recommendations regarding the Alert Aggregator:

1. All message originators will comply with the trust model when sending messages through the alert framework to the Alert Gateway. (see Section 8.1)
2. Alert Aggregator will be operated according to the requirements set forth in the trust model.
3. The authorized government entity will publish open non-proprietary standards for message origination
4. The Alert Aggregator will utilize CAP as the messaging standard to the Alert Gateway.
5. Messages will be delivered to the Alert Gateway on a first-in first-out basis, with the exception of the Presidential message, which will move to the front of any existing messages.
6. The Alert Aggregator will support bi-directional message traffic to deliver the message and to notify the alert message originator of the status of their CMAS message.
7. The Alert Aggregator may consist of separate paths for the delivery of the message to the Alert Gateway and from the Alert Gateway for message status notification.

2.2.3 Reference Point B

The actions to be performed by Reference Point B include the following:

1. Carry forward information for the authentication and validation of actions across this reference point.
2. Delivery of a new, updated, or cancelled wireless alert message to Alert Gateway in CAP format.
3. Carry acknowledgement from Alert Gateway to Alert Aggregator that the new, updated, or cancelled wireless alert message has been received.

2.2.4 Alert Gateway

2.2.4.1 General Alert Gateway System Requirements

The functions to be performed by the Alert Gateway include the following:

1. Ensure authenticity of interactions with the Alert Aggregator and the CMSP Gateway.
2. Validate (e.g., authentication and non-repudiation) the received wireless alert message.
3. Maintain a log of wireless alert messages received from the Alert Aggregator and delivered to and rejected by the CMSP Gateway.
4. Implementation and support of defined ‘service profiles’ specifying alert message formats containing information elements required by CMSPs for the delivery of alert messages to wireless devices.
5. Stores CMSPs profiles including the CMSP election within a specific service area, supported technologies including any associated service profiles, characteristics, restrictions, limitations, or parameters.
6. Deployment to achieve geographic separation from the CMSP Gateway.

7. Support interfacing with multiple CMSPs and multiple CMSP Gateways per CMSP.

8. Geographically redundant Alert Gateway to avoid a single point of failure.

2.2.4.2 CMSP Profile Support

The CMSAAC recommends that the Alert Gateway have a profile for every CMSP. The CMSAAC further recommends that these profiles be administered using the following procedures:

- The CMSP Gateway IP addresses and CMSP service area on a state level will be provided by an authorized CMSP representative to the Alert Gateway administrator 30 days in advance of the required in-service date when CMSP begin to transmit the CMAMs.

- Any updates of CMSP profile will be provided by an authorized CMSP representative to the Alert Gateway administrator in writing at least 30 days in advance of the required in-service date.

- The parties will negotiate and mutually agree on an implementation date.

Table 2-1 CMSP Profile on Alert Gateway

Profile Parameter	Parameter Election	Description
CMSP Name		Unique identification of CMSP
CMSP Gateway Address	IP address or Domain Name	
	Alternate IP address	Optional and subject to implementation
Geo-Location Filtering	<yes / no>	If “yes” the only CMAM issued in the listed states will be sent to the CMSP Gateway. If “no”, all CMAM will be sent to the CMSP Gateway.
If yes, list of states	CMAC Geocode for state	List can be state name, abbreviated state name, or CMAC GeoCode for state (see Section 10.4.5)

2.3 CMSP Administered Elements Definitions & Requirements

2.3.1 Reference Point C

The CMSAAC recommends that the actions to be performed by Reference Point C include the following:

1. Provide information for the authentication and validation of actions across this reference point.

2. Delivery of a new, updated, or cancelled wireless alert message by the Alert Gateway in a format that is suitable for the mobile devices and the wireless alert delivery technology or technologies implemented by the Commercial Mobile Service Provider.

3. Acknowledgement from CMSP Gateway to Alert Gateway that the new, updated, or cancelled wireless alert message has been received.

2.3.2 CMSP Gateway

The CMSAAC recommends that the functions to be performed by the Commercial Mobile Service Provider Gateway include the following:

1. Authentication of interactions with the Alert Gateway.
2. Management of Commercial Mobile Service Provider elections to support CMAS alert services within the Commercial Mobile Service Provider's service areas.
3. Determination if Commercial Mobile Service Provider has elected to offer CMAS alert services within the specified alerting area.
4. Determination of which delivery technology or delivery technologies will be utilized for the transmission of CMAS alert messages within the specified alerting area.
5. Map the alert area of the CMAS alert message into the associated set of cell sites / paging transceivers.
6. Manage and execute CMAS alert retransmission subject to delivery technology capability and CMSP policy.
7. A CMSP that elects to transmit alerts will have one or more CMSP Gateways designated for receipt of alerts from the Alert Gateway.
8. The CMSP Gateway should have redundancy and designed to provide high reliability and availability comparable to similarly situated network elements.
9. A Commercial Mobile Service Provider may have one or more CMSP Gateways in the CMSP network to support regional distribution of CMSA messages and to handle anticipated CMAM traffic levels. The CMSP has the responsibility for the distribution of the CMAM traffic among CMSP Gateways.
10. CMSP Gateway(s) in a CMSP network will be identified by a unique IP address or domain name.
11. The CMSP Gateway will support the defined CMAS "C" interface and associated protocols between the Alert Gateway and the CMSP Gateway.
12. The interface from the CMSP Gateway to the CMSP Infrastructure is Commercial Mobile Service Provider and technology dependent and is not specified in CMAS.
13. The CMSP Gateway model will support standardized IP based security mechanisms such as a firewall. The CMSP will provide a secure connection from the CMSP Gateway to the Alert Gateway for reception of the CMAS messages.
14. The CMSP Gateway application will support CMAM:
    a. Authentication
    b. Message integrity
    c. Availability (i.e. keep alive messages)
15. The CMSP Gateway will support a mechanism on the Reference Point C interface with the Alert Gateway to stop and start alert message deliveries from the Alert Gateway to the CMSP Gateway under conditions such as the event too many messages are being received on the interface, the CMSP Gateway buffers are full, congestion exists at the CMSP Gateway, etc.
16. The CMSP Gateway will support a mechanism to handle congestion within the CMSP Infrastructure according to CMSP policy.
17. The CMSP Gateway will not be responsible for performing any formatting, re-formatting, or translation of the CMAM other than the following:
    a. Text, audio, video, and multimedia files may require transcoding into the proper format (e.g., codec) supported by the mobile device.

18. The CMSP Gateway will be responsible for validating message integrity and alerting parameters and respond with an error message to the Alert Gateway if these validations fail.
19. The CMSP Gateway will retrieve any resources (e.g., audio, video, multimedia files such as graphics) from the Alert Gateway if the alert attributes indicate a resource is available and if the CMSP has the capability to broadcast these resource types.
20. The CMSP Gateway will process CMAMs in a first in – first out (FIFO) queuing method except for a Presidential-level alert which will be immediately moved to the top of the queue and processed before all other non-Presidential alerts.

2.3.3 CMSP Infrastructure

CMSP infrastructure functionality is generally dependent on delivery technology, the capabilities of the delivery technology, and mobile vendor/CMSP specific policy and requirements. The following are general guidelines recommended by the CMSAAC for the functions to be performed by the CMSP Infrastructure:

1. Authentication of interactions with the Mobile Device which is dependent upon the capabilities of the delivery technology and CMSP policy. This function may not be part of CMAS but a capability of the underlying delivery technology.
2. Distribute the received CMAS alert message to the determined set of cell sites/paging transceivers for transmission to the mobile devices within the range of cell sites/pager transceivers.
3. For each specified cell site/pager transceiver, transmit the CMAS alert message using the delivery technology or delivery technologies supported by the Commercial Mobile Service Provider for that specific cell site/paging transceiver.

2.3.4 Reference Points D & E

Reference Points D and E are defined and controlled by the Commercial Mobile Service Providers. The CMSAAC recommendations in this document define what type of information needs to be conveyed across Reference Point E to support CMAS alerts on mobile devices. The CMSAAC recommends that the definition of the Reference Point D and E protocols be performed by the commercial mobile service providers in conjunction with the CMSP infrastructure network vendors and the mobile device vendors.

2.3.5 Mobile Device

Mobile device functionality is generally dependent on delivery technology, the capabilities of the delivery technology, and mobile vendor/CMSP specific policy and requirements. CMAS should allow for mobile device vendor flexibility in the design of CMA user interactions, and allow for innovation by the mobile device vendors and CMSPs, especially as mobile device technology advances. The following are general guidelines recommended by the CMSAAC for the functions to be performed by the Mobile Device:

1. Authentication of interactions with the CMSP infrastructure. The authentication will not be part of the CMAS alert and is delivery technology dependent.
2. Determination of delivery technology or delivery technologies being supported by the Commercial Mobile Service Provider in the subscriber's current visited network.
3. Monitor associated channel or channels according to the requirements of the delivery technology or delivery technologies for CMAS alerts.
4. Maintain configuration of CMAS alert options including the following:
    a. Subscriber's choice of CMAS alert opt-out selections.
    b. Subscriber's preferred language for CMAS alerts if applicable to the delivery technology.
    c. Default language of English if CMAS alert is not being transmitted in subscriber's preferred language.

5. Extraction of the CMAS alert content in the subscriber's preferred language or in the default language of English, if the CMAS alert is not being transmitted in the subscriber's preferred language.
6. Presentation of received CMAS alert content to the mobile device user in accordance with the capabilities of the mobile device, if the CMAS alert complies with the subscriber's opt-out selections.
    a. Presidential level CMAS alerts are always presented.
    b. Presentation of a CMAS alert will activate associated visual, audio, and mechanical (e.g., vibration) indicators per subscriber options configured on the mobile device.
7. Detection and suppression of presentation of duplicate CMAS alerts.
8. Suppression of CMAS alert visual, audio and mechanical (e.g., vibration) indicators upon subscriber's action on the mobile device user interface (e.g., key stroke, touch screen).

3 Deployment Scenarios

The WARN Act specifies that a commercial mobile service operator who elects to transmit emergency alerts can elect to transmit the CMAS alerts in whole or in part {Sec. 602(b)(1)(B)}. The CMSAAC recommends that the definition of "in whole or in part" include the following:

- All or a subset of the CMSP's service area
- All or a subset of current and future mobile devices supported by the CMSP network

For reasons detailed in Annex B – WARN Act Statutory Requirements, the date of election is likely not the date of deployment. Therefore the CMSAAC recommends that the process for a CMSP to "file an election with the Commission with respect to whether or not it intends to transmit emergency alerts" should include the following information:

1. Potential date of initial deployment
2. Potential date when mobile device(s) with CMAS support are available for consumer purchase
3. Whether the deployment will be "in whole or in part"

It is important to understand the various scenarios that may be deployed in CMSP networks to support CMAS for those CMSP that do elect to transmit the CMAS alerts in whole or part. In addition, these scenarios need to be understood for the development of appropriate information a CMSP must provide to the subscriber to educate them on the availability of CMAS alerts. This information also needed to educate the sources of the CMAS alerts so there is not an unrealistic expectation as to the percentage of population to which the alert message may be broadcast.

Note: the following diagrams shows variety of mobile devices (i.e. cellular mobile phones and pagers) as illustrative examples; it is not the intention to suggest all mobile device technologies are supported by a single operator or via a single CMSP network.

3.1 Scenarios for Single Technology Deployed

3.1.1 Scenario – CMAS in Entire Single Technology Operator Network on All Devices

This scenario is where the CMSP deploys a single delivery technology within the CMSP network to support CMAS alerts, and all mobile devices on that network support the delivery technology and thus the reception of the CMAS alerts.

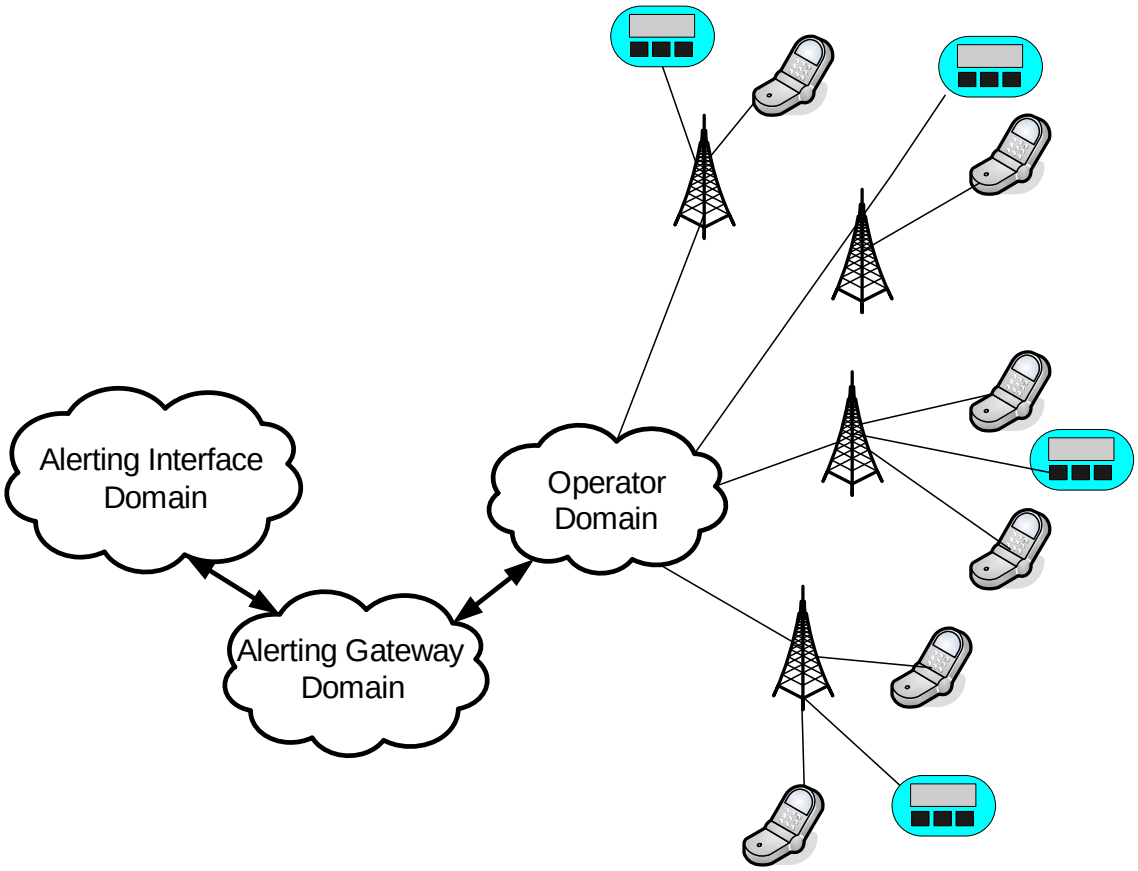

Figure 3-1 CMAS in Entire Single Technology Network on All Devices

3.1.2 Scenario – CMAS in Entire Single Technology Operator Network on a Subset of Devices

This scenario is where the CMSP deploys a single delivery technology within the CMSP network to support CMAS alerts, and only a subset of mobile devices on that CMSP network support the delivery technology and thus the reception of the CMAS alerts.

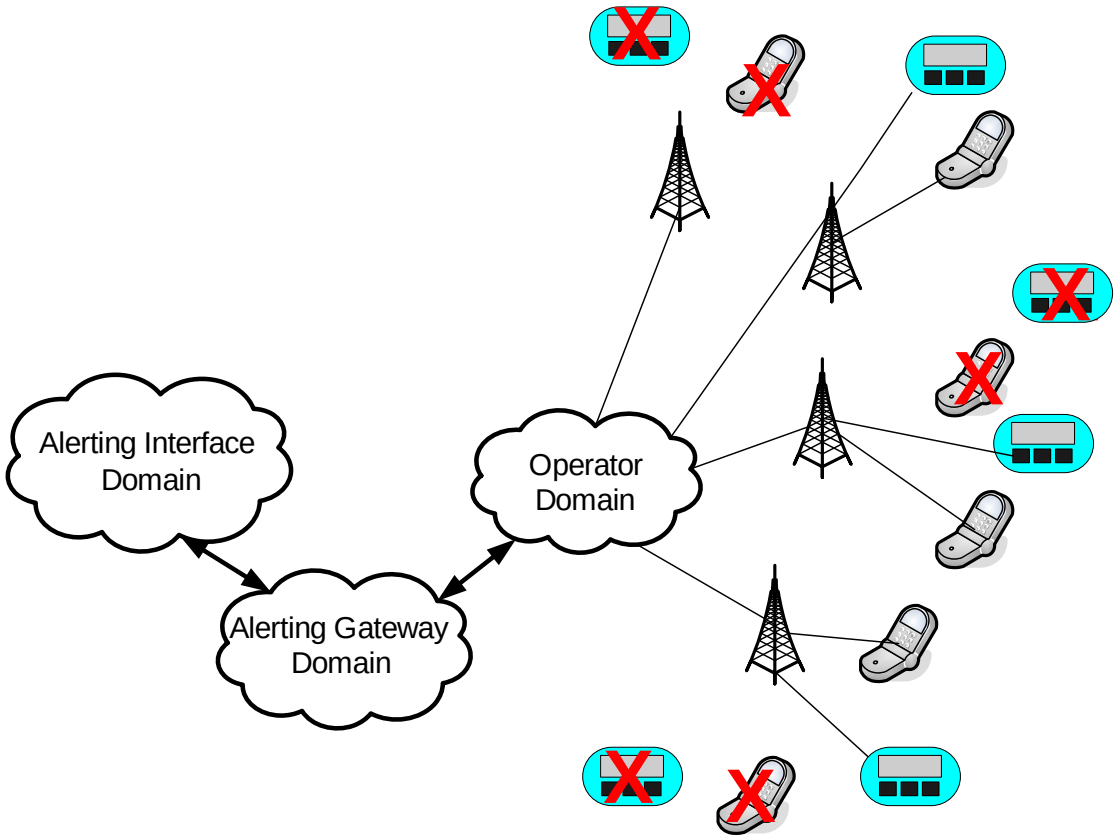

Figure 3-2 CMAS in Entire Network on Sub-set of Devices

3.1.3 Scenario – CMAS in Subset of Single Technology Operator's Network on All Devices

This scenario is where the CMSP deploys a single delivery technology in a subset of the CMSP network to support CMAS alerts, and all mobile devices on that CMSP network support the delivery technology and thus the reception of the CMAS alerts while in the portion of the CMSP network where the delivery technology is deployed.

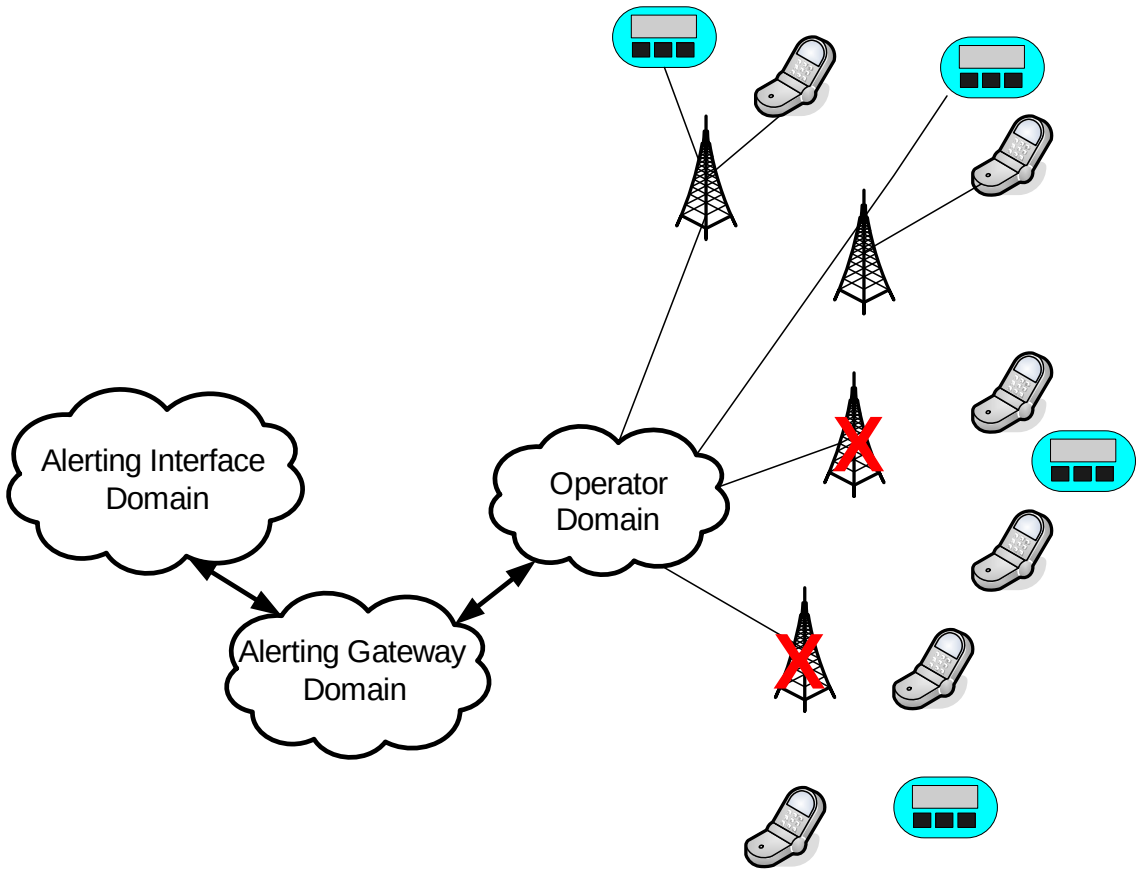

Figure 3-3 CMAS in Subset of Single Technology Operator's Network on All Devices

3.1.4 Scenario – CMAS in Subset of Single Technology Operator's Network on Subset of Devices

This scenario is where the CMSP deploys a single delivery technology in a subset of the CMSP network to support CMAS, and only a subset of mobile devices on the CMSP network support the delivery technology and thus the reception of the CMAS alerts while in the portion of the CMSP network where the delivery technology is deployed.

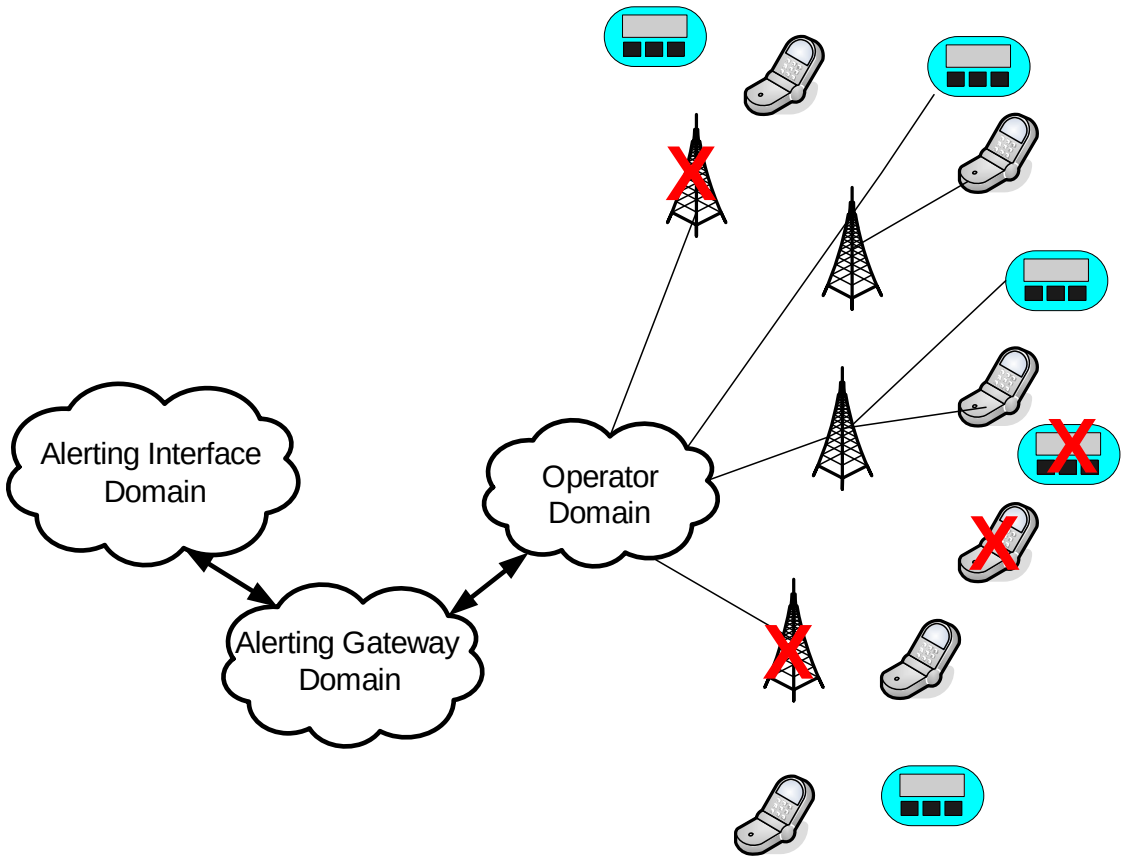

Figure 3-4 CMAS in Subset of Single Technology Operator's Network on Subset of Devices

3.2 Scenarios for Multiple Technologies Deployed

3.2.1 Scenario – CMAS in Entire Multiple Technology Operator Network on All Devices

This scenario is where the CMSP deploys a multiple delivery technologies within the CMSP network to support CMAS alerts, and all mobile devices on that CMSP network support all delivery technologies and thus the reception of the CMAS alerts.

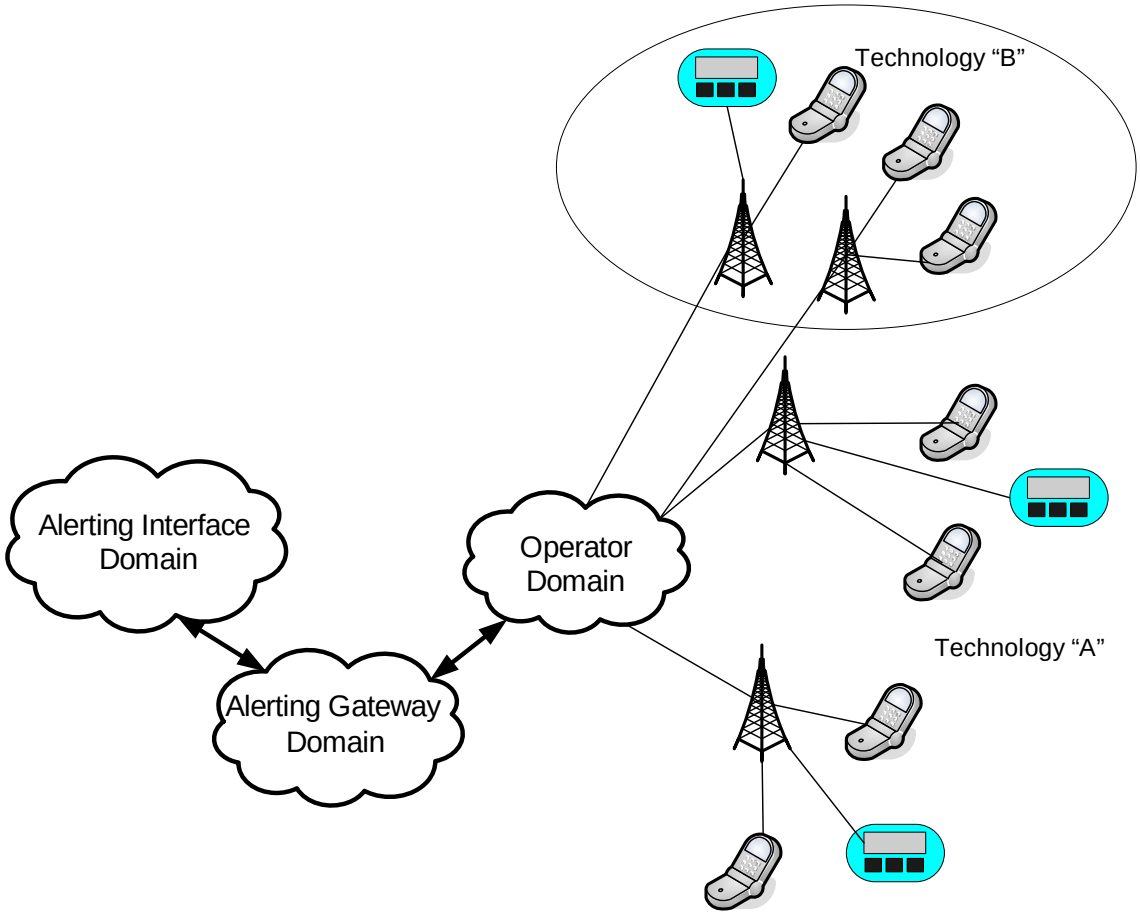

Figure 3-5 CMAS in Entire Multiple Technology Operator Network on All Devices

3.2.2 Scenario – CMAS in Entire Multiple Technology Operator Network on Subset of Devices

This scenario is where the CMSP deploys multiple delivery technologies within the CMSP network to support CMAS alerts, and only a subset of mobile devices on the CMSP network supports one or both delivery technologies and thus the reception of the CMAS alerts. Some mobile devices may not support either deliver technology.

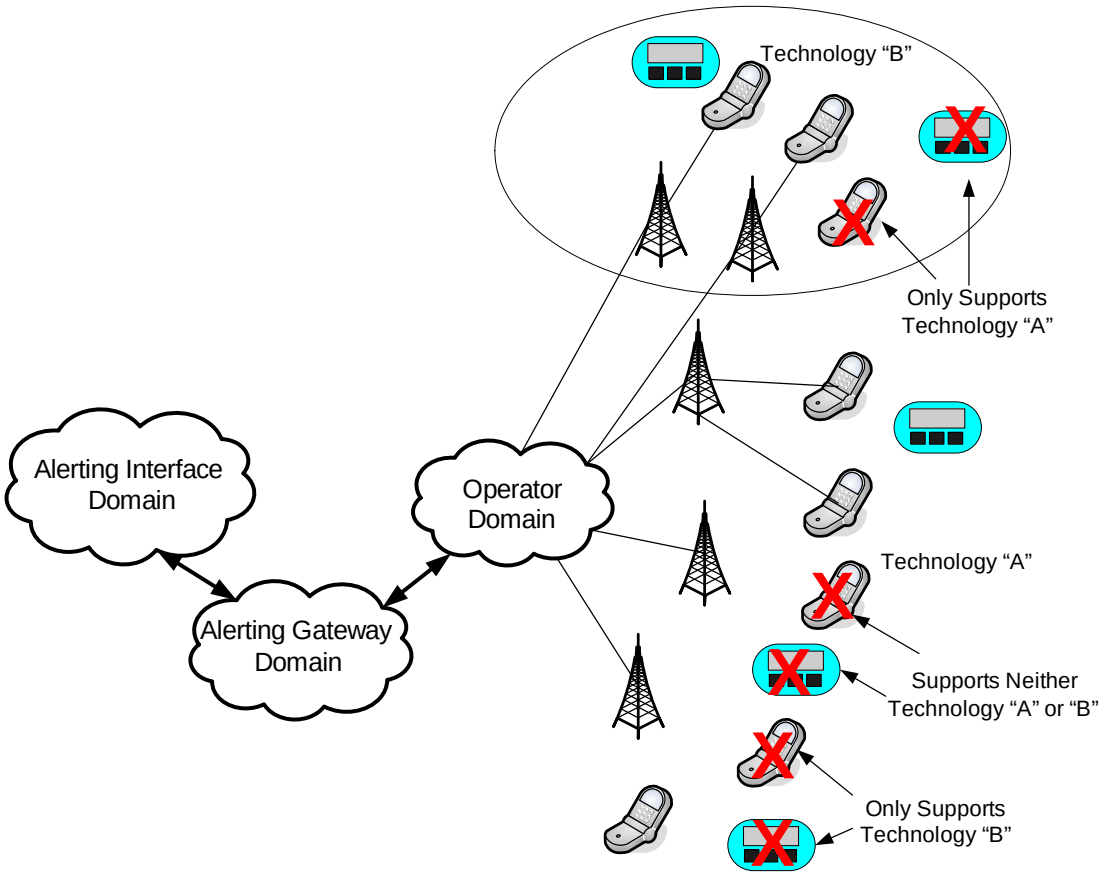

Figure 3-6 CMAS in Entire Multiple Technology Operator Network on Subset of Devices

3.2.3 Scenario – CMAS in Subset of Multiple Technology Operator Network on Subset of Devices

This scenario is where the CMSP deploys multiple delivery technologies on a subset of the CMSP network to support CMAS alerts, and only a subset of mobile devices on the CMSP network support one or both delivery technologies and thus the reception of the CMAS alerts. Some mobile devices may not support either delivery technology. This is a realistic picture of the deployment of CMAS, especially in a nationwide scenario.

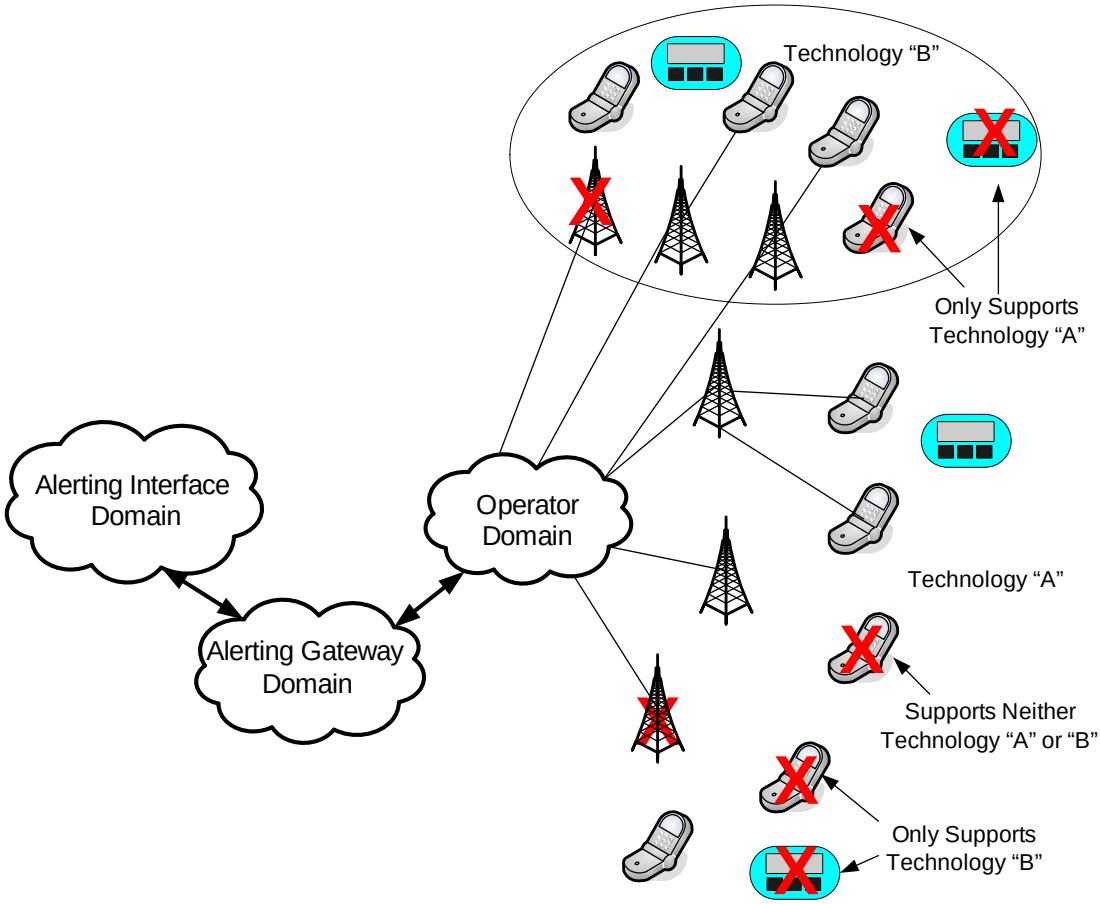

Figure 3-7 CMAS in Subset of Multiple Technology Operator Network on Subset of Devices

3.3 Scenario for Operator Does Not Elect to Transmit CMAS Alerts

This option is where the CMSP does not elect to transmit CMAS alerts.

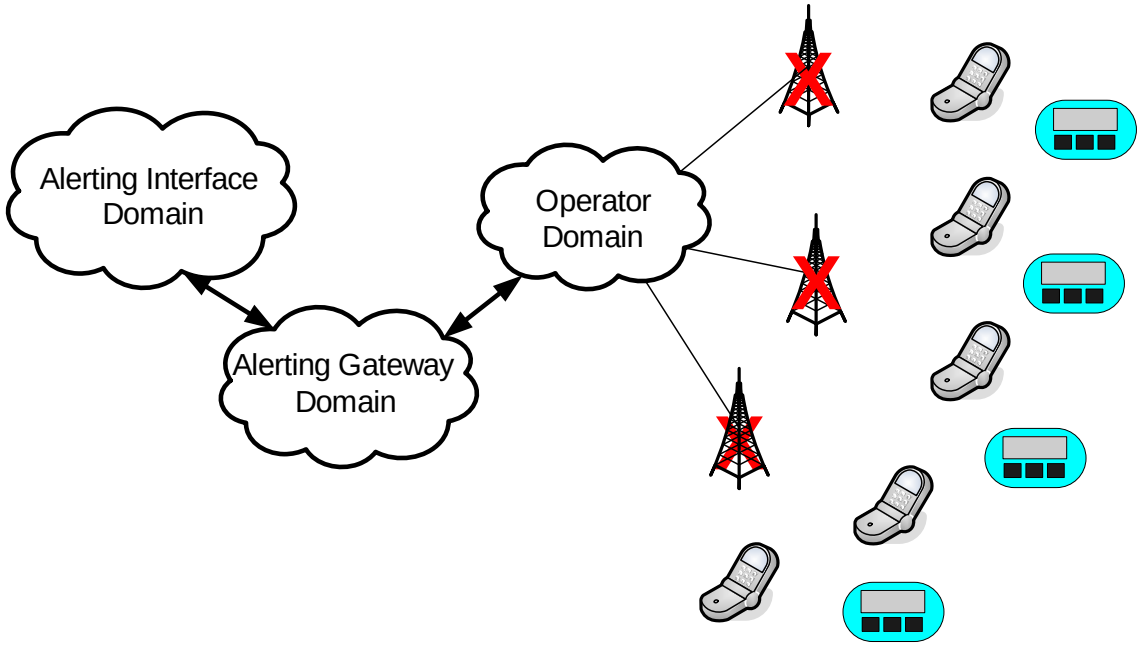

Figure 3-8 Operator Does Not Elect to Transmit CMAS Alerts

3.4 Subscriber Notification Recommendations

The CMSAAC, in collaboration with the Cellular Telephone and Internet Association (CTIA) and its membership developed the proposed text to be used by commercial mobile service providers to notify their subscribers 1) when they intend to transmit emergency alerts "in part" or 2) when they do not intend to transmit emergency alerts. The WARN Act appears not to require specific text be developed for service providers who elect to transmit emergency alerts throughout its entire coverage area. Therefore no text was developed for that case.

3.4.1 Notification Procedures

The Commercial Mobile Service Alert Advisory Committee (CMSAAC) recommends that carriers retain the discretion to determine how to provide specific information regarding (1) whether or not they offer wireless emergency alerts, and (2) which devices are or are not capable of receiving wireless emergency alerts, as well as how to tailor additional notice, if necessary, for devices offered at other points of sale, *i.e.*, retail outlets, mobile virtual network operators ("MVNOs") and third party vendors.

3.4.2 Notification Text Recommendations

The Commercial Mobile Service Alert Advisory Committee (CMSAAC) submits the following recommended notice text, consistent with the requirements of the WARN Act.

I. NOTICE BY CARRIER WHO INTENDS TO TRANSMIT EMERGENCY ALERTS "IN PART."

NOTICE REGARDING TRANSMISSION OF
WIRELESS EMERGENCY ALERTS (Commercial Mobile Alert Service)

[[WIRELESS PROVIDER]] has chosen to offer wireless emergency alerts within portions of its service area, as defined by the terms and conditions of its service agreement, on wireless emergency alert capable devices. There is no additional charge for these wireless emergency alerts.

Wireless emergency alerts may not be available in the entire service area or on all devices. For details on the availability of this service and wireless emergency alert capable devices, please ask a sales representative, or go to [[INSERT WEBSITE URL]].

Notice required by FCC Rule XXXX (Commercial Mobile Alert Service).

II. NOTICE BY CARRIER WHO, "IN WHOLE," DOES NOT INTEND TO TRANSMIT EMERGENCY ALERTS

NOTICE TO NEW AND EXISTING SUBSCRIBERS REGARDING TRANSMISSION OF WIRELESS EMERGENCY ALERTS (Commercial Mobile Alert Service)

[[WIRELESS PROVIDER]] presently does not transmit wireless emergency alerts.

Notice required by FCC Rule XXXX (Commercial Mobile Alert Service).

4 CMAS Alert Scenarios

This section provides descriptions recommended by the CMSAAC for many common scenarios which are related to the support of CMAS Alert messages. These scenarios are a representative sample and do not include all possible sequences and/or events. Specifically this section will include descriptions of the following scenarios:

- Nominal CMAS alert scenarios for text based CMAS alert, streaming audio or streaming video CMAS alert, and downloaded multimedia CMAS alerts
- CMAS alert cancellation scenario
- CMAS alert update scenarios for text based CMAS alert, streaming audio or streaming video CMAS alert, and downloaded multimedia CMAS alerts
- CMAS alert expiration scenario
- Duplicate CMAS alerts scenarios for both duplicate CMAS alerts on the same broadcast technology and duplicate CMAS alerts from different broadcast technologies
- Multiple different active CMAS alerts scenarios
- Multiple different CMAS alerts

4.1 Nominal CMAS Alert Scenarios

4.1.1 Scenario for Nominal Text CMAS Alert

An event has occurred and the appropriate government entities have decided to issue a text based Commercial Mobile Alert (CMA) to warn the Commercial Mobile Service Provider (CMSP) subscribers within the indicated alerting area.

This scenario applies to both the CMSP subscribers and to subscribers who are roaming as visiting subscribers into the service area of the CMSP network which will be broadcasting the CMA.

4.1.1.1 Pre-Conditions

1. Mobile device is authorized and authenticated for service on CMSP network.
2. Mobile device is receiving adequate radio signal strength from the CMSP.
3. Mobile device is in state that allows for the detection and reception of the CMA (e.g., not busy, not on a voice call).
4. No previous Commercial Mobile Alert Message (CMAM) being broadcast by the CMSP.
5. There is no active CMAM on mobile device.
6. CMSP subscriber is within the alerting area for the CMA.

4.1.1.2 Normal Flow

The normal flow for the text based CMA is described in the following steps and in the associated flow diagram which follows:

1. The appropriate government entity creates the alert message in CAP format which is sent to the government alerting network over Reference Point A.
2. The government alerting network validates and authenticates the received alert request.
    a. If the alert fails validation or authentication, an error response is returned to the originating government entity and the alert is not sent to the CMSP. End of scenario.

3. The government alerting network converts the received alert message into the text profile based CMAS format supported by the CMSP.
    a. If the alert fails conversion, the alert is not sent to the CMSP. End of scenario.
4. The text profile based CMAM is sent to the CMSP over Reference Point C.
5. The CMSP validates the received CMAM.
    a. If the CMAM fails validation, an error response is returned to the government alerting network and the CMAM is not broadcast by the CMSP. End of scenario.
6. The CMSP sends an acknowledgement to the government alerting network that a valid CMAM has been received.
7. The CMSP performs geo-targeting to translate the indicated alert area into the associated set of cell sites / paging transceivers for the broadcast of the CMA.
    a. If the CMSP does not support CMAS in the indicated alert area, the CMAM is not broadcast by the CMSP. End of scenario.
    b. If the CMSP does not have any cell site / paging transceiver coverage within the indicated alert area, the CMAM is not broadcast by the CMSP. End of scenario.
    c. If the entire nation is indicated as the alert area then all cell sites / paging transceivers of the CMSP which support the CMAS service are used for the broadcast of the CMAM.
8. The CMSP broadcasts the CMAM to the set of cell sites / paging transceivers identified by the geo-targeting processing in the previous step.
    a. The CMAM is broadcast via the CMSP selected technology.
9. The mobile device monitors for the broadcast of the CMAM via the CMSP selected technology.
    a. If the CMAM is not a Presidential alert and if the end user opt-out selections for CMAS alerts indicate that this type of CMAM is not to be presented, the CMAM is discarded or ignored. End of scenario.
10. The CMAM is received and presented to the end user including the activation of the CMAS audio attention signal and/or the activation of the special emergency alert vibration cadence (if mobile device has vibration capabilities) for a short duration as defined by CMSP policies and by the capabilities of the mobile device, and display of the CMAM message text on the visual display of the mobile device.
    a. Activation of the CMAS audio attention signal and/or special vibration cadence complies with the end user mobile device configuration as defined in Section 7.3.
11. The behavior of the mobile device beyond this point is outside the scope of the WARN Act and, therefore, is not subject to recommendations by the CMSAAC. The functionality of the mobile device is CMSP and mobile device specific.

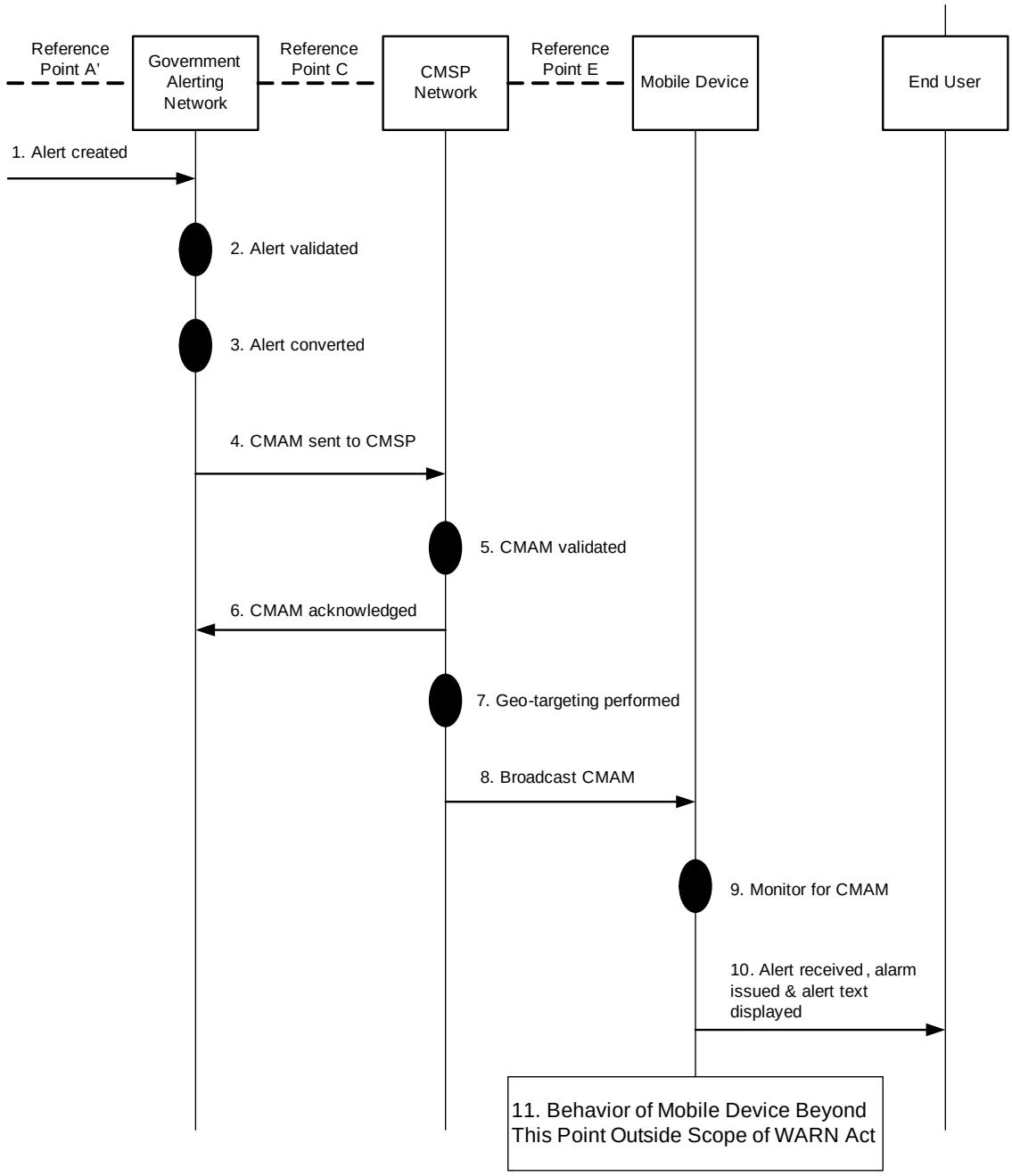

Figure 4-1 Flow for Scenario for Nominal Text CMAS Alert

4.1.2 Scenario for Nominal Streaming Audio or Streaming Video CMAS Alert

Streaming audio or streaming video CMAS alerts are a future capability.

4.1.3 Scenario for Nominal Downloaded Multimedia CMAS Alert

Downloaded multimedia CMAS alerts are a future capability.

4.2 CMAS Alert Cancellation Scenario

The event that caused the issuance of the Commercial Mobile Alert (CMA) has changed and the appropriate government entities have decided that the event is no longer an imminent threat to life or property. Consequently the appropriate government entities have decided to issue a cancellation of the CMA.

This scenario applies to both the Commercial Mobile Service Provider (CMSP) subscribers and to subscribers who are roaming as visiting subscribers into the service area of the CMSP network which will be broadcasting the CMA.

If the received CMAM cancellation is not valid and if, as a part of its implementation, the CMSP has enabled message retransmission, the CMSP may continue to send the original alert until expiry or until a valid CMAM cancellation is received.

4.2.1 Pre-Conditions

1. Mobile device is authorized and authenticated for service on CMSP network.
2. Mobile device is receiving adequate radio signal strength from the CMSP.
3. Mobile device is in state that allows for the detection and reception of the CMA (e.g., not busy, not on a voice call).
4. A previous non-expired Commercial Mobile Alert Message (CMAM) has been broadcast by the CMSP and has been received by the mobile device.
5. There is an active CMAM on mobile device.
6. CMSP subscriber is within the alerting area of the active CMA.

4.2.2 Normal Flow

The normal flow for the cancelled CMA is described in the following steps and in the associated flow diagram which follows:

1. The appropriate government entity creates the alert cancellation message in CAP format which is sent to the government alerting network over Reference Point A.
2. The government alerting network validates and authenticates the received alert cancellation request.
    a. If the alert fails validation or authentication, an error response is returned to the originating government entity and the alert cancellation is not sent to the CMSP. End of scenario.

3. The government alerting network converts the received alert message into the text profile based CMAS format support by the CMSP
    a. The Alert Gateway ensures that the urgency, severity, certainty match the values of those fields in the original message. As a consequence, a cancelled CMAM passed to the CMSP Gateway has the same urgency, severity, certainty, and message category as the original CMA alert in order to ensure the opt-out filter on the handset is the same for both messages. Therefore if the original CMAM was ignored based on opt-out criteria, then the CMAM cancellation should also be ignored.
    b. If the alert fails conversion, the alert cancellation is not sent to the CMSP. End of scenario.

4. The CMAM cancellation is sent to the CMSP over Reference Point C.
5. The CMSP validates the received CMAM cancellation.
    a. If the CMAM cancellation fails validation, an error response is returned to the government alerting network and the CMAM cancellation is not broadcast by the CMSP. End of scenario.
6. The CMSP sends an acknowledgement to the government alerting network that a valid CMAM cancellation has been received.
7. The CMSP discontinues the broadcasts the associated CMAM including the text component and any associated audio, video, or multimedia components.
8. The CMSP performs geo-targeting to translate the indicated alert area into the associated set of cell sites / paging transceivers for the broadcast of the CMA.
    a. If the CMSP does not support CMAS in the indicated alert area, the CMAM is not broadcast by the CMSP. End of scenario.
    b. If the CMSP does not have any cell site / paging transceiver coverage within the indicated alert area, the CMAM is not broadcast by the CMSP. End of scenario.
    c. If the entire nation is indicated as the alert area then all cell sites / paging transceivers of the CMSP which support the CMAS service are used for the broadcast of the CMAM.
9. The CMSP broadcasts the CMAM cancellation to the same set of cell sites / paging transceivers identified by the geo-targeting processing in the previous step.
10. The mobile device monitors for the broadcast of the CMAM cancellation via the CMSP selected technology and receives the CMAM cancellation.
    a. If the CMAM cancellation is not a Presidential alert and if the end user opt-out selections for CMAS alerts indicate that this type of CMAM is not to be presented, the CMAM cancellation is discarded or ignored. End of scenario.
11. The CMAM cancellation is received and the CMAM cancellation is presented to the end user including the activation of the CMAS audio attention signal and/or the activation of the special emergency alert vibration cadence (if mobile device has vibration capabilities) for a short duration as defined by CMSP policies and the capabilities of the mobile device, and the display of the CMAM cancellation message text on the visual display of the mobile device.
    a. Activation of the CMAS audio attention signal and/or special vibration cadence will comply with the end user mobile device configuration as defined in Section 7.3.
12. The behavior of the mobile device beyond this point is outside the scope of the WARN Act and, therefore, is not subject to recommendations by the CMSAAC. The functionality of the mobile device is CMSP and mobile device specific.

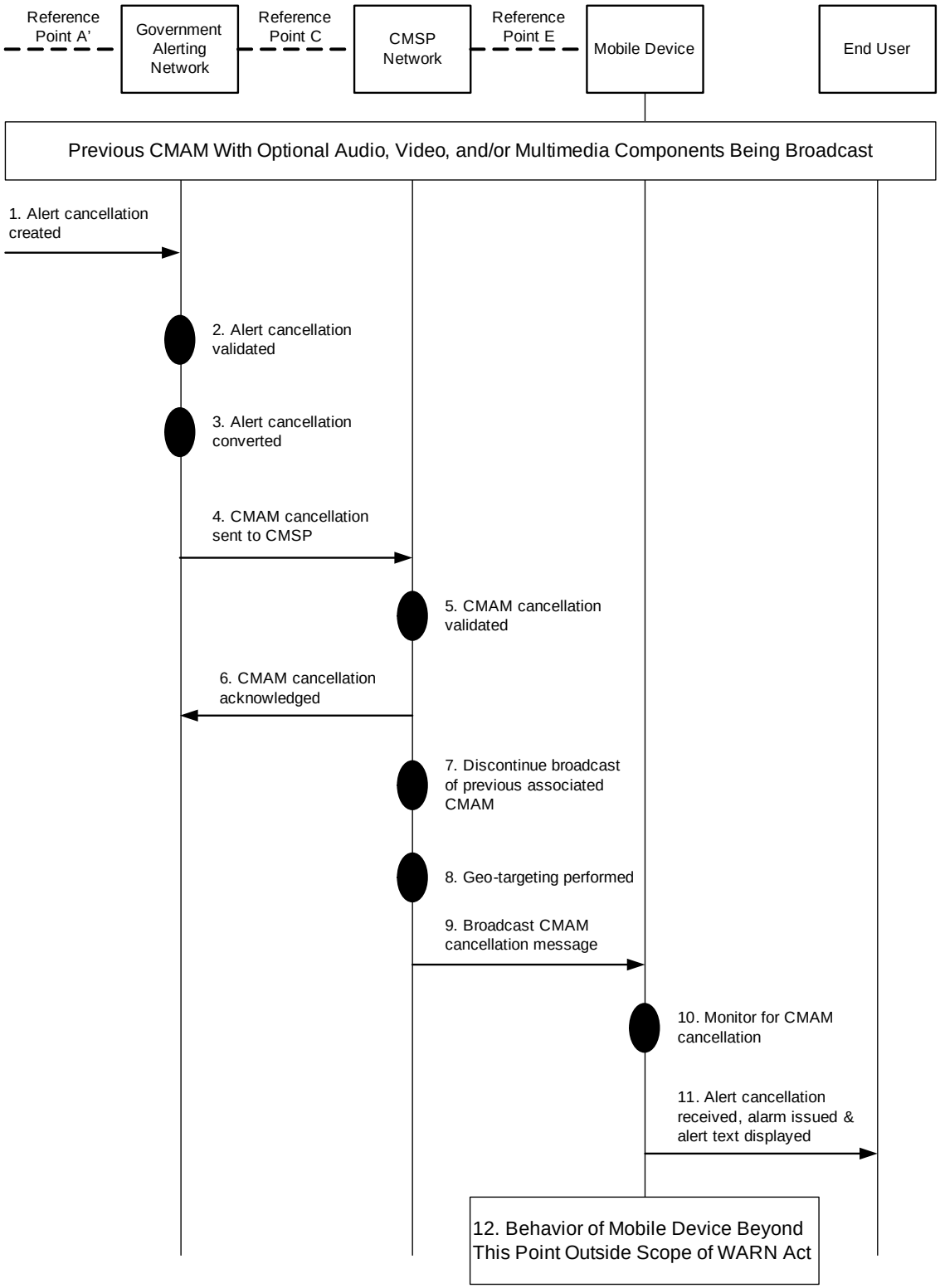

Figure 4-2 Flow for CMAS Alert Cancellation Scenario

4.3 CMAS Alert Update Scenarios

4.3.1 Scenario for Update of Text CMAS Alert

The appropriate government entities have decided to issue an update to a previously issued text based Commercial Mobile Alert (CMA) to warn the Commercial Mobile Service Provider (CMSP) subscribers within the indicated alerting area about changes associated with the event that caused the issuance of the previous CMA.

This scenario applies to both the CMSP subscribers and to subscribers who are roaming as visiting subscribers into the service area of the CMSP network which will be broadcasting the CMA.

If the received CMAM cancellation is not valid and if, as a part of its implementation, the CMSP has enabled message retransmission, the CMSP may continue to send the original alert until expiry or until a valid CMAM cancellation is received.

4.3.1.1 Pre-Conditions

1. Mobile device is authorized and authenticated for service on CMSP network.
2. Mobile device is receiving adequate radio signal strength from the CMSP.
3. Mobile device is in state that allows for the detection and reception of the CMA (e.g., not busy, not on a voice call).
4. The CMSP may be broadcasting a previous CMA which is associated with the updated CMA.
5. A CMAM may be active on mobile device.
6. CMSP subscriber is within the alerting area of the updated CMA.

4.3.1.2 Normal Flow

The normal flow for the update of text based CMAM is described in the following steps and in the associated flow diagram which follows:

1. The appropriate government entity creates the updated alert message in CAP format which is sent to the government alerting network over Reference Point A.
2. The government alerting network validates and authenticates the received updated alert request.
    a. If the alert fails validation or authentication, or conversion, an error response is returned to the originating government entity and the alert is not sent to the CMSP. End of scenario.
3. The government alerting network converts the received alert message into the text profile based CMAS format supported by the CMSP.
    a. The Alert Gateway ensures that the urgency, severity, certainty match the values of those fields in the original message. As a consequence, an updated CMAM passed to the CMSP Gateway has the same urgency, severity, certainty, and message category as the original CMA alert in order to ensure the opt-out filter on the handset is the same for both messages. Therefore if the original CMAM was ignored based on opt-out criteria, then the updated CMAM should also be ignored.
    b. If the alert fails conversion, the alert is not sent to the CMSP. End of scenario.
4. The updated text based CMAM is sent to the CMSP over Reference Point C.
5. The CMSP validates the received updated CMAM.
    a. If the updated CMAM fails validation, an error response is returned to the government alerting network and the updated CMAM is not broadcast by the CMSP. End of scenario.
6. The CMSP sends an acknowledgement to the government alerting network that a valid updated CMAM has been received.

7. The CMSP discontinues any broadcasts of the previously issued CMAM.
8. The CMSP performs geo-targeting to translate the indicated alert area into the associated set of cell sites / paging transceivers for the broadcast of the updated CMAM.
    a. If the CMSP does not support CMAS in the indicated alert area, the updated CMAM is not broadcast by the CMSP. End of scenario.
    b. If the CMSP does not have any cell site / paging transceiver coverage within the indicated alert area, the updated CMAM is not broadcast by the CMSP. End of scenario.
    c. If the entire nation is indicated as the alert area then all cell sites / paging transceivers of the CMSP which support the CMAS service are used for the broadcast of the updated CMAM.
9. The CMSP broadcasts the updated CMAM to the set of cell sites / paging transceivers identified by the geo-targeting processing in the previous step.
    a. The updated CMAM is broadcast via the CMSP selected technology.
10. The mobile device monitors for the broadcast of the updated CMAM via the CMSP selected technology.
    a. If the updated CMAM is not a Presidential alert and if the end user opt-out selections for CMAS alerts indicate that this type of CMAS alert is not to be presented, the updated CMAM is discarded or ignored. End of scenario.
11. The updated CMAM is received and presented to the end user including the activation of the CMAS audio attention signal and/or the activation of the special emergency alert vibration cadence (if mobile device has vibration capabilities) for a short duration as defined by CMSP policies and the capabilities of the mobile device, and the display of the updated CMAM message text on the visual display of the mobile device.
    a. Activation of the CMAS audio attention signal and/or special vibration cadence complies with the end user mobile device configuration as defined in Section 7.3.
12. The behavior of the mobile device beyond this point is outside the scope of the WARN Act and, therefore, is not subject to recommendations by the CMSAAC. The functionality of the mobile device is CMSP and mobile device specific.

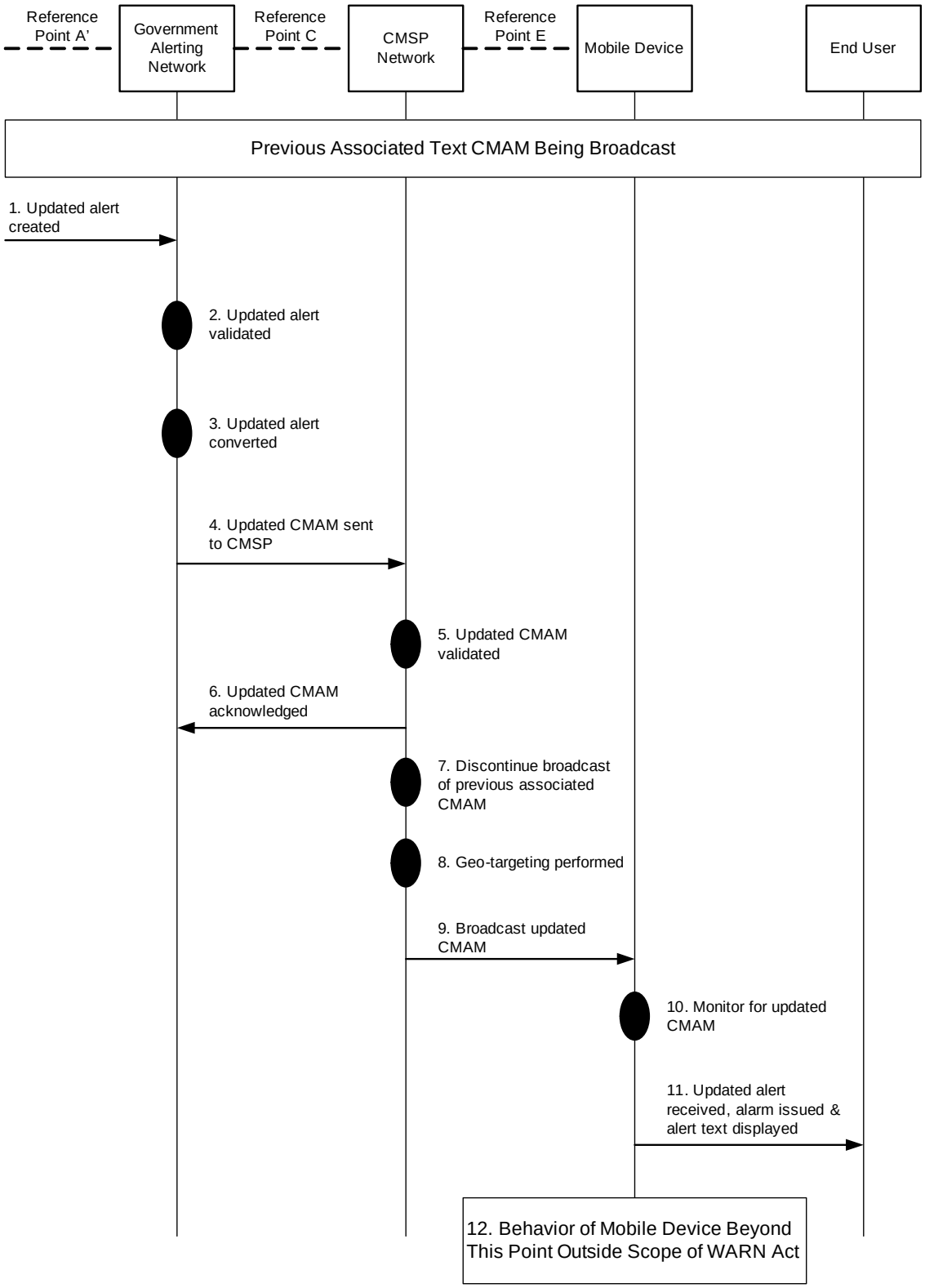

Figure 4-3 Flow for Scenario for Update of Text CMAS Alert

4.3.2 Scenario for Update of Streaming Audio or Streaming Video CMAS Alert

Streaming audio or streaming video CMAS alerts are a future capability.

4.3.3 Scenario for Update of Downloaded Multimedia CMAS Alert

Downloaded multimedia CMAS alerts are a future capability.

4.4 CMAS Alert Expiration Scenario

The previously issued Commercial Mobile Alert Message (CMAM) alert has reached its expiration time without having been updated or cancelled. This scenario describes the functionality when the expiration time has been detected.

4.4.1 Pre-Conditions

1. The associated non-expired non-cancelled CMAM has been or is currently being broadcast by the Commercial Mobile Service Provider (CMSP).

4.4.2 Normal Flow

The normal flow for the CMAS alert expiration is described in the following steps and in the associated flow diagram which follows:

1. The expiration time of a previously issued CMAM has been determined by the CMSP.
2. Any active broadcasts of text component of the previously issued CMAM are discontinued by the CMSP.
3. All active broadcasts of any associated audio, video, or multimedia components of the previously issue CMAM are discontinued by the CMSP.

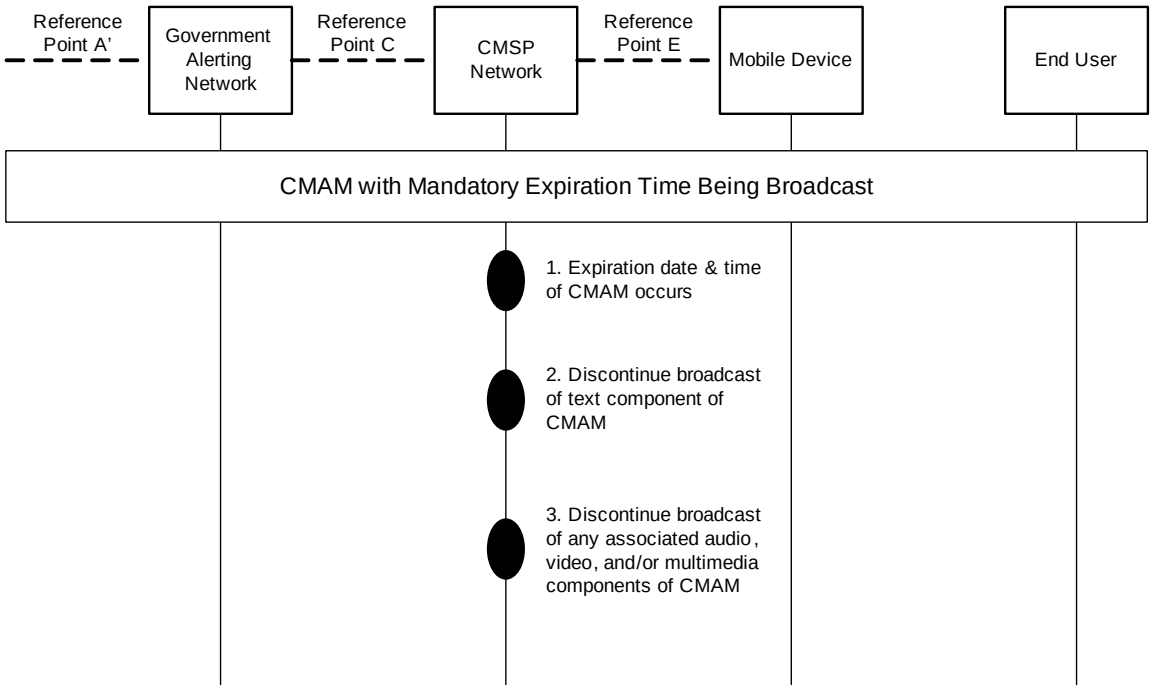

Figure 4-4 Flow for CMAS Alert Expiration Scenario

4.5 Duplicate CMAS Alerts Scenarios

4.5.1 Scenario for Duplicate CMAS Alerts on Same Broadcast Technology

A Commercial Mobile Alert Message (CMAM) is being retransmitted by the CMSP network. The mobile device detects and ignores the duplicate CMAM.

This scenario applies to both the Commercial Mobile Service Provider (CMSP) subscribers and to subscribers who are roaming as visiting subscribers into the service area of the CMSP network which will be broadcasting the Commercial Mobile Alert (CMA).

4.5.1.1 Pre-Conditions

1. Mobile device is authorized and authenticated for service on CMSP network.
2. Mobile device is receiving adequate radio signal strength from the CMSP.
3. Mobile device is in state that allows for the detection and reception of CMAM (e.g., not busy, not on a voice call).
4. A previous copy of the CMAM has been broadcast by the CMSP.
5. The previous copy of the CMAM is contained on mobile device.
6. CMSP subscriber is still within the alerting area for the CMA.

4.5.1.2 Normal Flow

The flow for duplicate CMAM on the same broadcast technology is described in the following steps and in the associated flow diagram which follows:

1. The CMSP network retransmits a previously broadcast CMAM.
   a. The CMAM being retransmitted contains the same message identifier as the previously broadcast version.
   b. The retransmission could be performed by the CMSP selected delivery technology depending on the capabilities of the delivery technology.
2. The mobile device monitors for the broadcast of the CMAM via the CMSP selected technology.
3. The mobile device detects the received CMAM as a duplicate CMAM based upon message identifier and other message attributes. The duplicate CMAM is ignored and discarded by the mobile station.

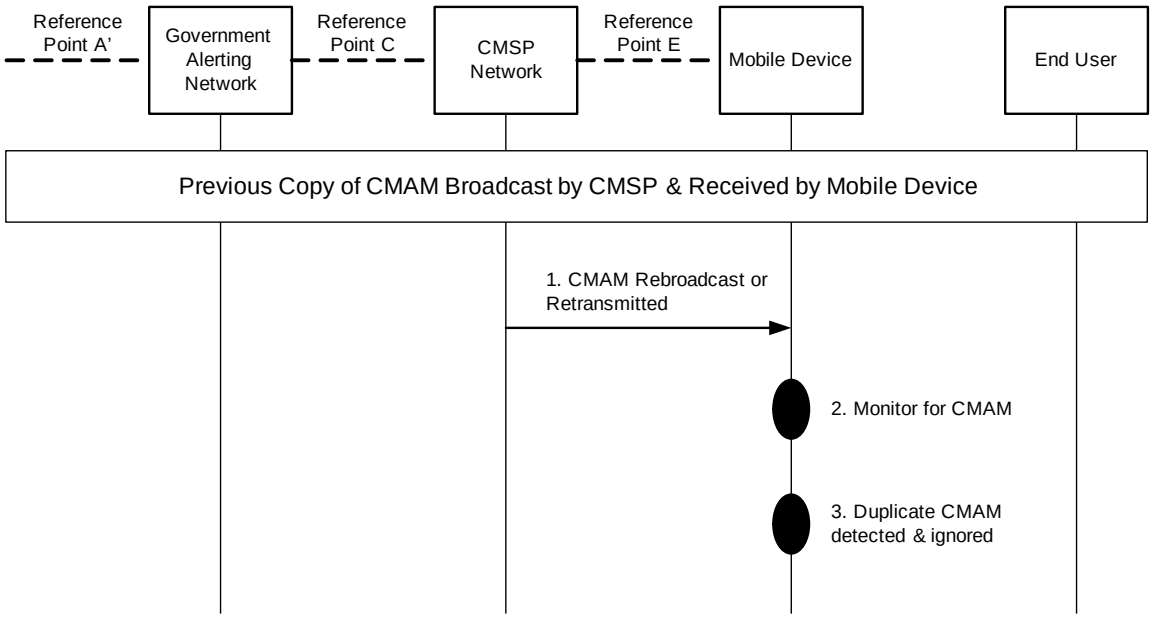

Figure 4-5 Flow for Scenario for Duplicate CMAS Alerts on Same Broadcast Technology

4.5.2 Scenario for Duplicate CMAS Alerts on Different Broadcast Technologies

An event has occurred and the appropriate government entities have decided to issue a text based Commercial Mobile Alert (CMA) to warn the Commercial Mobile Service Provider (CMSP) subscribers within the indicated alerting area. The CMSP network supports more than one broadcast technology in the indicated alerting area and the CMSP elects to broadcast the CMA on more than one technology in the indicated alerting area.

Support of multiple broadcast technologies by the CMSP network may be result of the deployment and implementation of newer broadcast technologies.

This scenario applies to both the CMSP subscribers and to subscribers who are roaming as visiting subscribers into the service area of the CMSP network which will be broadcasting the CMA.

4.5.2.1 Pre-Conditions

1. Mobile device is authorized and authenticated for service on CMSP network.
2. Mobile device is receiving adequate radio signal strength from the CMSP.

3. Mobile device is in state that allows for the detection and reception of the CMA (e.g., not busy, not on a voice call).
4. No previous Commercial Mobile Alert Message (CMAM) is being broadcast by the CMSP.
5. There is no active CMAM on mobile device.
6. CMSP subscriber is still within the alerting area for the CMA.
7. The mobile device is capable of receiving the CMAM from more than one broadcast technology.

4.5.2.2 Normal Flow

The flow for duplicate text profile based CMAS alerts on the different broadcast technologies is described in the following steps and in the associated flow diagram which follows:

1. The appropriate government entity creates the alert message in CAP format which is sent to the government alerting network over Reference Point A.
2. The government alerting network validates and authenticates the received alert request.
    a. If the alert fails validation or authentication, an error response is returned to the originating government entity and the alert is not sent to the CMSP. End of scenario.
3. The government alerting network converts the received alert message into the text profile based CMAS format supported by the CMSP.
    a. If the alert fails conversion, the alert is not sent to the CMSP. End of scenario.
4. The text profile based CMAM is sent to the CMSP over Reference Point C.
5. The CMSP validates the received CMAM.
    a. If the CMAM fails validation, an error response is returned to the government alerting network and the CMAM is not broadcast by the CMSP. End of scenario.
6. The CMSP sends an acknowledgement to the government alerting network that a valid CMAM has been received.
7. The CMSP performs geo-targeting to translate the indicated alert area into the associated set of cell sites / paging transceivers for the first broadcast technology used for the broadcast of the CMAM.
    a. If the CMSP does not support CMAS in the indicated alert area, the CMAM is not broadcast by the CMSP. End of scenario.
    b. If the CMSP does not have any cell site / paging transceiver coverage for the first broadcast technology within the indicated alert area, the CMAM is not broadcast by the CMSP using the first broadcast technology. The CMAM will be processed as described in Section 4.1.1 . End of scenario.
    c. If the entire nation is indicated as the alert area then all cell sites / paging transceivers of the first broadcast technology of the CMSP which support the CMAS service are used for the broadcast of the CMAM.
8. The CMSP broadcasts the CMAM using the first broadcast technology to the set of cell sites / paging transceivers identified by the geo-targeting processing in the previous step.
    a. The CMAM is broadcast via the first CMSP selected technology.
9. The CMSP performs geo-targeting to translate the indicated alert area into the associated set of cell sites / paging transceivers for the second broadcast technology used for the broadcast of the CMAM.
    a. If the CMSP does not have any cell site / paging transceiver coverage for the second broadcast technology within the indicated alert area, the CMAM is not broadcast by the CMSP using the second broadcast technology. The CMAM is processed as described in Section 4.1.1. End of scenario.

c. If the entire nation is indicated as the alert area then all cell sites / paging transceivers of the second broadcast technology of the CMSP which support the CMAS service are used for the broadcast of the CMAM.

10. The CMSP broadcasts the CMAM using the second broadcast technology to the set of cell sites / paging transceivers identified by the geo-targeting processing in the previous step.

    a. The CMAM is broadcast via the second CMSP selected technology.

11. The CMAM is received from both the first and second broadcast technologies.

12. Based upon mobile device capabilities and configurations, only one of the received CMAM will be presented to the end user. The mobile device should only perform one activation of the CMAS audio attention signal and/or the activation of the special emergency alert vibration cadence (if mobile device has vibration capabilities).

    a. If the CMAM is not a Presidential alert and if the end user opt-out selections for CMAS alerts indicate that this type of CMAS alert is not to be presented, the CMAM is discarded or ignored. End of scenario.

13. The behavior of the mobile device beyond this point is outside the scope of the WARN Act and, therefore, is not subject to recommendations by the CMSAAC. The functionality of the mobile device is CMSP and mobile device specific.

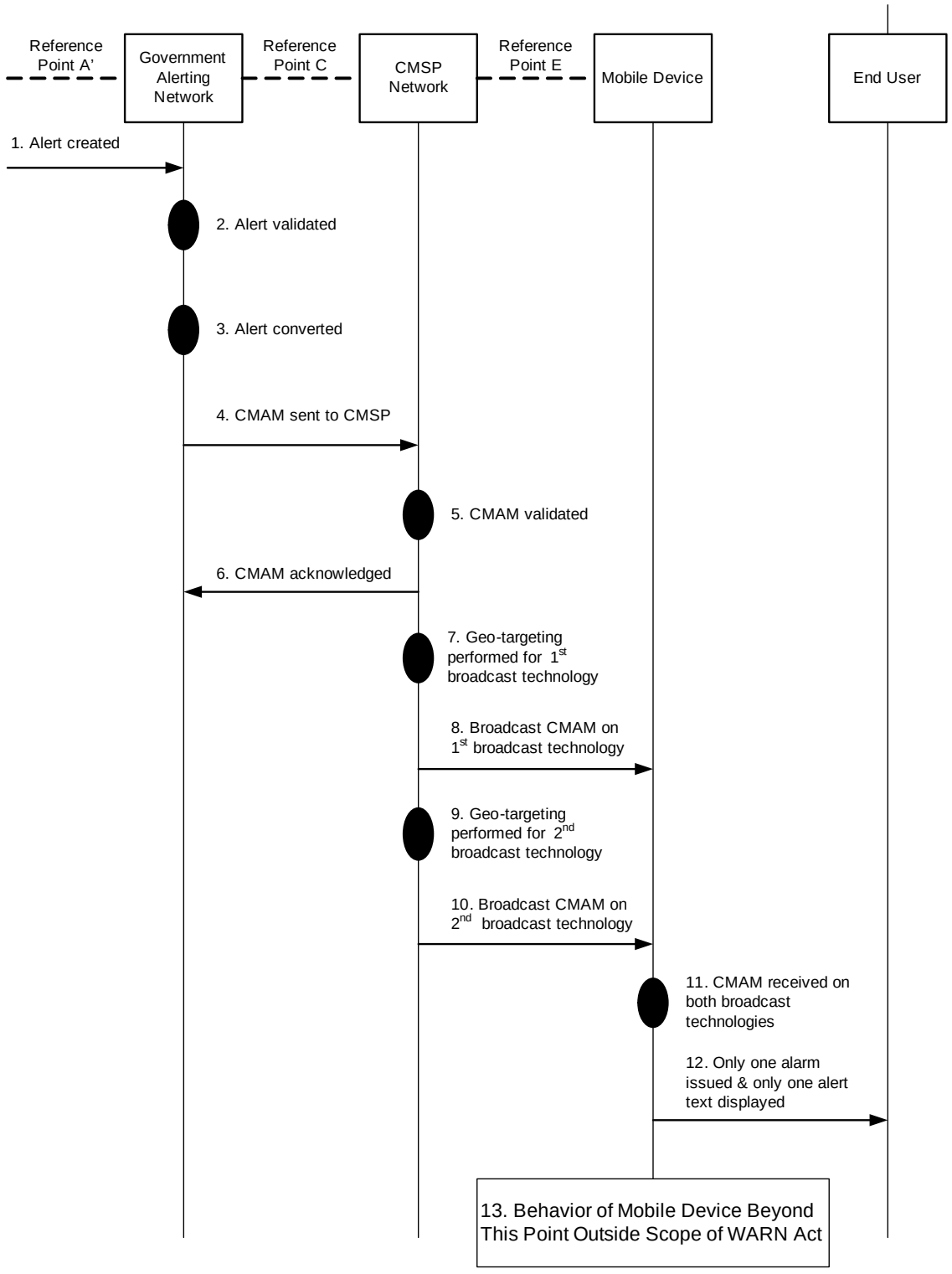

Figure 4-6 Flow for Scenario for Duplicate CMAS Alerts on Different Broadcast Technologies

4.6 Multiple Different Active CMAS Alerts Scenario

An event has occurred and the appropriate government entities have decided to issue a text based Commercial Mobile Alert (CMA) to warn the Commercial Mobile Service Providers (CMSP) subscribers within the indicated alerting area. During the broadcast period of the 1st alert message, a second event has occurred for the same alerting area and the appropriate government entities have decided to issue a second text based CMA to warn the CMSP subscribers within the indicated alerting area.

The CMSP processes CMAM received from the Alert Gateway on a first come first served basis. There is no prioritization of processing or delivery of CMAM within the CMSP network.

This scenario applies to both the CMSP subscribers and to subscribers who are roaming as visiting subscribers into the service area of the CMSP network which will be broadcasting the CMA.

4.6.1 Pre-Conditions

1. Mobile device is authorized and authenticated for service on CMSP network.
2. Mobile device is receiving adequate radio signal strength from the CMSP.
3. Mobile device is in state that allows for the detection and reception of CMA (e.g., not busy, not on a voice call).
4. No previous Commercial Mobile Alert Message (CMAM) being broadcast by the CMSP.
5. There is no CMAM on mobile device.
6. CMSP subscriber is within the alerting area for the CMA.
7. Both CMA are to be issued for the same alerting area.

4.6.2 Normal Flow

The flow for multiple different CMAS alerts within the same alerting area is described in the following steps and in the associated flow diagram which follows:

1. The appropriate government entity creates the 1st alert message in CAP format which is sent to the government alerting network over Reference Point A.
2. The government alerting network validates and authenticates the 1st received alert request.
    a. If the 1st alert fails validation or authentication, an error response is returned to the originating government entity and the alert is not sent to the CMSP. End of scenario.
3. The government alerting network converts the 1st received alert message into the text profile based CMAS format supported by the CMSP.
    a. If the alert fails conversion, the alert is not sent to the CMSP. End of scenario.

4 The 1st text profile based CMAM is sent to the CMSP over Reference Point C.

5. The CMSP validates the 1st received CMAM.
    a. If the 1st CMAM fails validation, an error response is returned to the government alerting network and the CMAM is not broadcast by the CMSP. End of scenario.
6. The CMSP sends an acknowledgement to the government alerting network that the 1st received CMAM is valid.
7. The CMSP performs geo-targeting for the 1st CMAS alert to translate the indicated alert area into the associated set of cell sites / paging transceivers for the broadcast of the 1st CMAM.
    a. If the CMSP does not support CMAS in the indicated alert area, the 1st CMAM is not broadcast by the CMSP. End of scenario.

b. If the CMSP does not have any cell site / paging transceiver coverage within the indicated alert area, the 1st CMAM is not broadcast by the CMSP. End of scenario.

c. If the entire nation is indicated as the alert area then all cell sites / paging transceivers of the CMSP which support the CMAS service are used for the broadcast of the 1st CMA.

8. The CMSP broadcasts the 1st CMAM to the set of cell sites / paging transceivers identified by the geo-targeting processing in the previous step.

   a. The 1st CMAM is broadcast via the CMSP selected technology.

9. The 1st CMAM is received and presented to the end user including the activation of the CMAS audio attention signal and/or the activation of the special emergency alert vibration cadence (if mobile device has vibration capabilities) for a short duration as defined by CMSP policies and by the capabilities of the mobile device, and display of the 1st CMAM message text on the visual display of the mobile device.

   a. If the 1st CMAM is not a Presidential alert and if the end user opt-out selections for CMAS alerts indicate that this type of CMAS alert is not to be presented, the CMAM is discarded or ignored.

   b. Activation of the CMAS audio attention signal and/or special vibration cadence complies with the end user mobile device configuration as defined in Section 7.3.

10. An appropriate government entity creates a 2nd alert message in CAP format for the same alerting area as the 1st alert message. The 2nd alert message is sent to the government alerting network over Reference Point A.

11. The government alerting network validates and authenticates the 2nd received alert request.

    a. If the 2nd alert fails validation or authentication, an error response is returned to the originating government entity and the alert is not sent to the CMSP. End of scenario.

12. The government alerting network converts the 2nd received alert message into the text profile based CMAS format supported by the CMSP.

    a. If the alert fails conversion, the alert is not sent to the CMSP. End of scenario.

13. The 2nd text profile based CMAM is sent to the CMSP over Reference Point C.

14. The CMSP validates the 2nd received CMAM.

    a. If the 2nd CMAM fails validation, an error response is returned to the government alerting network and the CMAM is not broadcast by the CMSP. End of scenario.

15. The CMSP sends an acknowledgement to the government alerting network that the 2nd received CMAM is valid.

16. The CMSP performs geo-targeting for the 2nd CMAM to translate the indicated alert area into the associated set of cell sites / paging transceivers for the broadcast of the 2nd CMAM.

    a. For this scenario, since the indicated alert area of the 1st and 2nd CMAM are the same, the results of the geo-targeting for both the 1st and 2nd CMAM should return the same set of cell sites / paging transceivers.

17. The CMSP broadcasts the 2nd CMAM to the set of cell sites / paging transceivers identified by the geo-targeting processing step.

    a. The 2nd CMAM is broadcast via the CMSP selected technology.

    b. The retransmission of the 1st CMAM and the initial transmission of the 2nd CMAM may be simultaneously broadcast, or may be transmitted sequentially, depending on the delivery technology

18. The 2nd CMAM is received and presented to the end user including the activation of the CMAS audio attention signal and/or the activation of the special emergency alert vibration cadence (if mobile device has vibration capabilities) for a short duration as defined by CMSP policies and by the capabilities of

the mobile device, and display of the 2nd CMAM message text on the visual display of the mobile device.

a. If the 2nd CMAM is not a Presidential alert and if the end user opt-out selections for CMAS alerts indicate that this type of CMAS alert is not to be presented, the 2nd CMAM is discarded or ignored.

b. Activation of the CMAS audio attention signal and/or special vibration cadence complies with the end user mobile device configuration as defined in Section 7.3.

c. The mobile device ignores the retransmission of the duplicate 1st CMAM.

d. The mobile device processing and presentation of multiple received CMAS alerts is outside the scope of the WARN Act and, therefore, is not subject to recommendations by the CMSAAC. The functionality of the mobile device is CMSP and mobile device specific

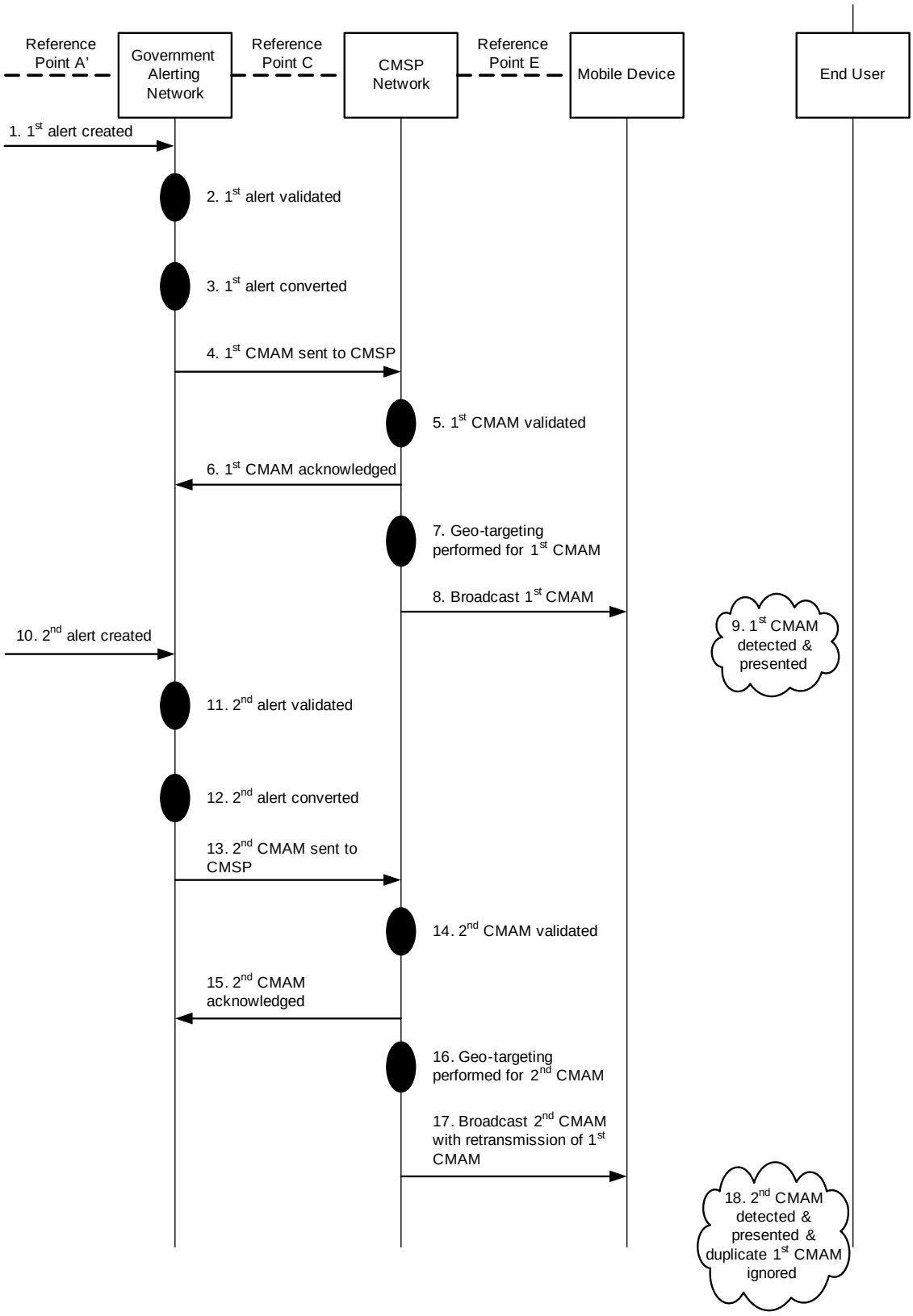

Figure 4-7 Flow for Scenario for Multiple Different Active CMAS Alerts Scenario

5 General Requirements & Conclusions

The following section contains the CMSAAC's general recommendations and conclusions for the CMAS. Many of the conclusions and recommendations apply to initial deployments of the CMAS, for a text-based service profile. Future technologies, such as streaming audio, streaming video, and multimedia, are mentioned throughout this document; however, technology advances to support these future capabilities are just beginning to be developed and introduced. As CMSPs gain experience with these technologies, the applicability of those technologies to the CMAS will be better understood.

The CMSAAC recommends that this document be treated as a living document, with periodic updates to account for experiences with initial CMAS deployments and experiences with new technologies and their applicability to CMAS. An industry group consisting of government and industry stakeholders should be created after the CMSAAC's activity is complete to review and update this document on a periodic basis. This review should occur no less frequently than biennially.

5.1 Scope & Definition of CMAS Alerts

The CMSAAC recommends that there are three classes of Commercial Mobile Alerts:

1. Presidential-level
2. Imminent threat to life and property (defined as alerts where the CAP severity equals Extreme or Severe, CAP urgency is Immediate or Expected, and CAP certainty is Observed or Likely.)
3. Child Abduction Emergency or "AMBER Alert"

Because of the technical limitations in delivering emergency alerts on CMSP systems, the CMSAAC recommends that only the 3 classes defined above will be transmitted as Commercial Mobile Alert (CMA) messages.

The CMSAAC recommends that the CMSPs who elect to support CMAs are considered for this purpose only to be agents of the federal, state, local, or tribal agencies that originate the alerts and are providing CMAs on their behalf.

The CMSAAC recommends that, prior to the adoption of rules as specified in the WARN Act section 602 (b) (1), the Commission will require all participants in the Commercial Mobile Service Alert Advisory Committee (CMSAAC) and all participants in the public comment process on this Commercial Mobile Alert Service Architecture and Requirements document to provide written assurance to the Commission that, if and insofar as one or more licenses may be required under any of their respective Intellectual Property Rights (IPR) that are technically essential for purposes of implementing or deploying CMAS, the rights holders shall license such IPR on a fair, reasonable and nondiscriminatory basis for those limited purposes only.

5.2 General CMAS Requirements & Conclusions

This section contains the CMSAAC's recommendations for general requirements and assumptions for CMAS. More specific requirements and assumptions may be contained within the other sections of this document.

1. Federal, state, tribal, and local level CMAS alert messages will be supported using the same CMAS solution.
2. Point-to-point or unicast delivery technologies are not feasible or practical for the support of CMAS, i.e. SMS point-to-point, MMS. Reasons for point-to-point technologies not being feasible or practical are:
    a. Point-to-point technologies can experience significant delivery delays.

b. Point-to-point technologies can result in network and radio interface congestion to the point of blocking voice calls.

c. Point-to-point technologies lack security and can be easily spoofed.

d. Point-to-point technologies lack geo-targeting capabilities because it is targeted to phone numbers instead of a specific alert area.

e. Point-to-point technologies lack emergency alert specific alert tones and thereby emergency alerts can not be distinguished from normal SMS message traffic.

f. Point-to-point technologies lack support of roamers

3. For a CMSP that elects to transmit CMAS alerts, text is the minimum requirement for CMAS alert messages. All CMAS alert messages delivered to the CMSP will contain at least a textual component.

4. No new CALEA lawful intercept access points will be created for CMAS alert broadcast delivery technologies.

5. There is no interaction between CMAS alert message delivery and Number Portability. There is no guarantee that the end user will receive the CMAS alert message during the time interval that the user's subscription is being ported between CMSPs. As part of Number Portability, there is no service portability between CMSPs.

6. It is not a requirement to support CMAS on non-initialized mobile devices, including mobile devices that are not authorized for service.

7. CMAS is intended for commercial mobile services (i.e, cellular phones and pagers) supported by commercial mobile service licensees. Some devices are not designed to support CMAS (e.g., telematics, data only devices such as laptop data cards) and thus are outside the scope of the CMAS architecture.

   a. Broadcast technologies such as MediaFLO and DVB-H are not considered as part of the CMAS. Service providers of these technologies do not hold commercial mobile service licenses as they do not provide interconnect service, and are not licensed to transmit in the same channels as commercial mobile services. It is recognized that these technologies may provide supplemental alert information for the CMAS.

8. The CMAMs are delivered across Reference C to the CMSP network at no cost to the CMSP.

5.3 Recommendations for Alert Initiation & Alert Initiators

5.3.1 CMAM Elements

A typical emergency alert message issued by the National Weather Service on weather radio might appear as follows:

"The National Weather Service in Phoenix has issued a severe thunderstorm warning for northwest Maricopa County effective until 5pm local time. Seek shelter now inside a sturdy structure and stay indoors!"

(Note the above message contains over 200 characters and spaces and is not in the correct format for a CMAM).

The CMSAAC recommends that CMAMs follow this same general format, within the text character limitations of CMA as defined in the text profile in Section 6.26.2. The necessary elements of an effective CMAM and the order in which they should be presented in the CMAM are:

1. What's Happening (Event Type or Event Category)

2. Area affected (in this area)

3. Recommended action (Response description)
4. Expiration time with time zone (Represented as a distinct time – e.g., until 09:30 AM EDT)
5. Sending Agency (agency type, i.e. police, fire, national weather service, etc.)

NOTE: The above format for a CMAM is recommended for initial deployments of CMAS and as experience is gained by alert initiators and by CMSPs, we envision that the format will evolve to provide to the most efficient and informative format for the CMAMs.

5.3.2 Generating CMAM from CAP Fields

For initial CMAS system deployments and until Alert Initiators are trained in the generation of CMAM, in order to create consistent and accurate CMAMs, the CMSAAC recommends that the Alert Gateway "construct" the CMAM using selected required and optional fields in the CAP message. The translated CMAM will then be transmitted to the CMSP across the C reference point.

Allowing the Alert Gateway to create the CMAM using CAP fields create consistent and accurate messages will enable enhancements to be made over time in the Alert Gateway and made available to all CMA capable mobile devices in the field. For instance, if a new alert event is identified, a new event code or category can be added to the CAP message, translated in the Alert Gateway and a new text string can be sent to the mobile device through the Commercial Mobile Service Provider (CMSP) Gateway.

However, generating CMAM using CAP fields may not provide flexibility to Alert Initiators to tailor the CMAM content to a specific alert event. Even though CMAS is not intended to provide comprehensive alert information, a CMAM with a "what is happening " text indicating "security warning" may not be very meaningful to the end user. The recent steam pipe explosion in New York City and the Virginia Tech shootings are examples where an automatically generated CMAM would not have provided meaningful information in the CMAM text.

The CMSAAC recommends the use of the sender identity used by the Alert Gateway in the trust model to identify the sender. The Alert Gateway will then assign an agreed upon text phrase or abbreviation (e.g., VDOT, NWS, etc.) to be transmitted to the CMSP Gateway.

The CMSAAC makes the following recommendations regarding the use of the required category and optional eventCode CAP fields. They are:

1. Encourage the National Weather Service to continue its practice of using codes, such as SAME codes, in the eventCode field to identify weather alerts.

2. When the eventCode field is populated with a value, that value will be used by the Alert Gateway to determine what text phrase will be transmitted to the CMSP gateway (e.g., TOR will be translated to Tornado Warning).

3. If the eventCode field is not populated or is populated with a value unknown to the Alert Gateway, the required category field will be used by the Alert Gateway to determine what text phrase to be transmitted to the CMSP gateway.

4. Emergency message originators and the National Weather Service are encouraged to utilize codes for eventCodes. These codes should be known by the Alert Gateway and have appropriate text phrases associated with them to be transmitted to the CMSP gateway. The CMSAAC recommends that a process be developed by which new event codes in addition to the standard SAME and CAP event codes can be developed and registered.

The CMSAAC recommends that the affected area be generated from the optional geocode field. If the optional geocode field is missing, the polygon or circle elements will be used to determine the associated geocodes and the corresponding affected area description. The CMSAAC further recommends that a

process be developed by which new geocodes in addition to standard FIPS codes can be registered and implemented in the Alert Gateway for deriving the affected area description.

The CMSAAC recommends that the response description will be taken from the optional responseType CAP Field. If the field is not populated, the message should be transmitted with the text string "Check local media for info" applied. The CMSAAC further recommends that a process be developed by which new responseType Codes in addition to the standard CAP response type codes can be developed and registered.

The CMSAAC recommends that the expiration time will be determined from the optional expires CAP field. If this field is not populated, local guidelines will be applied by the Alert Gateway as to when the message is no longer in effect.

The following table defines the text string associated with the CAP value fields used to generate the CMAM:

Table 5-1 CAP Value Field Mapping to Text

What is happening		
CAP Field	**Value**	**Text String**
category	Met	Severe Weather Warning
	Safety	Public Safety Warning
	Fire	Fire Warning
	Geo	Geologic Warning
	Security	Security Warning
	Rescue	Rescue Alert
	Health	Health Warning
	Env	Environmental Warning
	Transport	Transport Alert
eventCode	TOR	Tornado Warning
	VOW	Volcano Warning
	SVR	Severe TStorm Warning
	EQW	Earthquake Warning
	TSW	Tsunami Warning
	BZW	Blizzard Warning
	DSW	Dust Storm Warning
	FFW	Flash Flood Warning
	HWW	High Wind Warning
	HUW	Hurricane Warning
	TRW	Tropical Storm Warning
	WSW	Winter Storm Warning
	CFW	Coastal Flood Warning
	FLW	Flood Warning
	FRW	Fire Warning
	SMW	Special Marine Warning
	AVW	Avalanche Warning
	CDW	Civil Danger Warning
	CEM	Civil Emergency
	HMW	HazMat Warning
	LEW	Police Warning
	CAE	AMBER Alert
	NUW	Nuclear PowerPlant Warning
When the alert expires		
CAP Field	**Value**	**Text String**
expires	The expiry time of the	Translated by the Alert

	information of the alert message. The date and time is represented in [dateTime] format (e. g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT).	Gateway to an event expires time in a 12 hour/Time zone format (i.e., Until7:00AM PDT)
What action should be taken		
CAP Field	**Value**	**Text String**
responseType	Shelter or SPW	Take Shelter Now
	Evacuate or EVA	Evacuate Now
	Prepare	Prepare for Action
	Execute	Execute Action
	Monitor	Check News Media For Info
What area is effected		
CAP Field	**Value**	**Text String**
areaDesc		
polygon	Optional element. The paired values of points defining a polygon that delineates the affected area of the alert message	Translated by the Alert Gateway to the name of the county receiving the message and sent as a county name (i.e., Fairfax County)
circle	Optional element. The paired values of a point and radius delineating the affected area of the alert message	Translated by the Alert Gateway to the name of the county receiving the message and sent as a county name (i.e., Fairfax County)
geocode	Optional element. The geographic code delineating the affected area of the alert message	Translated by the Alert Gateway to the name of the county receiving the message and sent as a county name (i.e., Fairfax County)
Who is sending the alert		
CAP Field	**Value**	**Text String**
sender	Identifies the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet domain name - could also come from the sender's name in the trust model.	Translated by the Alert Gateway to an acronym or short abbreviation picked by the sender Note: URLs, phone numbers, and email addresses are not sent to the mobile device.

5.3.2.1 Generating CMAM from Free Form Text

As indicated in the above section, the generation of CMAM using CAP fields may not provide flexibility to Alert Initiators to tailor the CMAM content to a specific alert event where only an event category is available such as a "security warning". In addition, Alert Initiators may want to provide specific response information above what is available in the CAP responseType field.

The CMSAAC recommends that a capability be provided for Alert Initiators to generate free form text consistent with the text profile of Section 6.2. The CMSAAC further recommends that the Alert Gateway have a mechanism to determine when the free form text should be used instead of the automatically

generated CMAM described in Section 5.3.2. The Alert Gateway mechanism is subject to the implementation of the Alert Gateway and the policy of the authorized government entity.

The CMSAAC recommends that the FCC establish a forum that includes the CMSPs to develop the Alert Gateway mechanism and policy for free form text-based CMAMs that will be subject to final approval of the CMSPs. This policy would encompass specific decision points at the Alert Gateway such as: the message length does not exceed the maximum character limit, the message contains no phone numbers or URLs which would encourage mass access of the wireless network, the message contains all the necessary elements of an effective message referenced in section, etc. If any of the decision points are not met, the automatically generated message would be issued to the CMSP instead of the free form text.

The CMSAAC recommends that the Alert Gateway issue automatically generated CMAMs for alerts other than presidential and AMBER Alert messages until free form CMAMs meet the policies established for the Alert Gateway.

If the use of free form text messages becomes problematic or induces network disruptions in practice, the Alert Gateway mechanism and policy would need to be modified to further restrict the issuance of free form text messages or to utilize only automatically generated CMAMs.

The free form text for the CMAM should be included as a parameter of the CAP message with the valueName indicating “CMAMtext”.

The CMSAAC further recommends that training be provided to Alert Initiators on generation of meaningful CMAM which provides sufficient information on the mobile devices. It is recommended that the above mentioned forum participate in the development of the training program for free form text targeted for CMAMs.

5.3.3 Presidential Message and AMBER Alert

There are two additional special cases where automatic text generation at the Alert Gateway would not be practical. These are the Presidential Alert message and AMBER Alerts. The CMSAAC recommends that:

1. They may be identified by either by a code in the optional CAP eventCode field – EAN for Presidential Alert and CAE for AMBER Alert - or by the required CAP sender field. Presidential level messages are not restricted to nationwide only alert messages. The Presidential level message may contain polygon, circle, GNIS, or geocode information to designate the targeted alert area.

2. The free text message would be presented to the Alert Gateway in a free text CAP field. This free text message would be transmitted to the CMSP gateway. For Presidential alerts, the Alert Gateway may use a generic statement such as “The President has issued an emergency alert. Check local media for more details”.

3. It may be desirable for some AMBER Alert messages to include specific information such as a vehicle license plate. The National Center for Missing and Exploited Children (NCMEC) should be authorized to formulate unique free-form message text for CMAS.

4. These two special cases will use the normal processes for sending messages to the Alert Aggregator (i.e., use of CAP messages) and will be treated as any other emergency alert initiated message except as specified above and in Section 2.2.2.

5.3.4 Recommended Message Initiator Training

In order for emergency message initiators to develop and transmit effective emergency messages, within the character length limits of the CMAM, the CMSAAC recommends that alert initiator training on

consistently populating CAP fields and generating CMAM be accomplished via the credentialing process (See Section 8.1).

5.4 Recommendations for Geo-Targeting of CMAS Alerts

The CMSAAC acknowledges that it is the goal of the CMAS for CMSPs to be able to deliver geo-targeted alerts to the areas specified by the Alert Initiator. Systems used by Alert Initiators may allow them to define an alert area on a map. For example, the defined alert area could include the projected path of a tornado or an event that encompasses a portion of an urban area. The CMSAAC further recognizes that CMSPs currently have limited capability to deliver geo-targeted alerts.

Based upon current capabilities, the CMSAAC recommends the following for geo-targeting of CMAS alerts:

1. In order to expedite initial deployments of CMAS an alert that is specified by a geocode, circle or polygon (see Section 10.4) will be transmitted to an area not larger than the CMSP's approximation of coverage for the county[5] or counties with which that geocode, circle, or polygon intersects. Some wireless technology RF propagation areas, for systems such as paging systems or multi-county cell sites, may greatly exceed a single county. In these instances, CMSPs will support geo-targeting subject to the limitations imposed by their technology. Cell sites' / paging transceivers' physical location within the alert area may be used to determine the initial predefined alert areas. The CMSP is not required to perform RF coverage mapping of cell sites / paging transceivers to initial alert areas.

    a. A CMSP may elect to target smaller areas. CMSP may elect to target CMAM for distributions to predefined alert areas smaller than a county and may use GNIS codes, polygon, or circle information to identify a predefined list of cell sites / paging transceivers within the alert area. In the interim period before the availability of dynamic targeting, the CMSAAC recommends that certain urban areas with populations exceeding 1,000,000 inhabitants or with other specialized alerting needs be identified for priority consideration regarding implementation of more precise geo-targeting. The CMSAAC further recommends that a process be established by the Alert Gateway operator and the CMSPs to identify no later than August 2008 those initial areas that should be given such priority treatment for more precise geo-targeting. The CMSAAC recognizes the desire to move forward with this process on a small number of areas with particularly urgent alerting needs as soon as possible. The CMSAAC recommends that Section 604 funding be provided to FEMA for this purpose.

2. The CMSAAC recognizes that the use of predefined sets of cell sites frequently will not optimally cover the alert area desired. Therefore, the CMSAAC recommends that the FCC encourage DHS/FEMA, in concert with CMSPs, to immediately initiate the research, development, testing, and evaluation program referenced in section 604 of the WARN Act. Section 604 requires DHS to establish a program to develop innovative technologies that will allow CMSPs to efficiently transmit geo-targeted CMAMs to the public. The CMSAAC further recommends that CMSPs work with this DHS program to evaluate the feasibility and implementation issues associated with proposed solutions to increase geographic targeting specificity. Finally, the CMSAAC recommends that the FCC assess the progress of the CMSP geo-targeting as part of the biennial review process.

3. The architecture to support CMAS shall not require the CMSPs to open the configuration, interfaces and topology of their network including cell or paging transceiver towers to any third parties, nor provide subscriber information or data outside their network. A CMSP shall not be required to report cell site / paging transceiver information, coverage information, or any RF properties of their respective networks. The CMSP shall be the sole agent responsible for determining which network facilities, elements, or locations are involved in transmitting an alert to a mobile device.

[5] County, parish or equivalent jurisdictional area.

4. Transmission of alerts shall be to two-dimensional areas. There shall not be any altitude or ceiling component.

5.5 Requirements and Recommendations on Needs of Users, Including Individuals with Disabilities and the Elderly

The WARN Act requirements for the establishment of the Commercial Mobile Service Alert Advisory Committee membership specifically call for representation from "national organizations representing individuals with special needs, including individuals with disabilities and the elderly". [6]

During its work, the CMSAAC reviewed input from members on accessibility considerations. Most of the following requirements benefit *all* subscribers in an emergency.

It is recognized that not all wireless devices have the features to support all recommendations, but manufacturers are strongly encouraged to implement those recommendations that are technically feasible, so that their mobile devices can accommodate as many users as possible for emergency alerting.

5.5.1 General Requirements

In order to notify mobile service subscribers that an emergency alert message has been received on the mobile device, the CMSAAC recommends that the CMAS support a common audio attention signal and a common vibrating cadence to be used solely for CMAMs. These alerting mechanisms must be distinct from all other audio alerting signals and vibrations available in the mobile device and must not be able to be selected or modified by the user for any other purpose. The CMAS audio attention signals and vibration cadence signals as defined in Section 7.2 are applicable to all mobile devices which support CMAS including any specialized mobile devices for individuals with special needs.

In addition, the CMSAAC recommends that the user should not be required to remember or use a unique command to turn off the notification of the CMAM. A familiar command, consistent with the other commands used for call or message handling on the mobile device, is recommended.

5.5.2 User Needs Requirements

5.5.2.1 Alert/Attention Signal

A unique vibration cadence (if supported by the mobile device) should be provided as well as a unique audio attention signal. If both are available, the two modes do not need to be activated simultaneously but will follow the user's settings in the handset. If the handset supports dual activation the signals will be simultaneous according to user settings, but otherwise will be separate signals. The vibration cadence for the alert signal should be noticeably different from the default cadence of the handset.

For devices that have polyphonic capabilities, the CMSAAC recommends that the audio attention signal should consist of more than one tone, all of which are to be in the low frequency range below 2 kHz, and

[6] Beyond the WARN Act, consideration may be given to legislation such as Title II of the Americans With Disabilities Act which requires accessibility to state and local government programs and communications; Section 504 of the Rehabilitation Act which requires accessibility of Federal government programs; Section 255 of the Communications Act which requires accessibility in telecommunications products where readily achievable; and Section 508 which applies to Federal government purchase of wireless devices.

preferably below 1 kHz. For devices which have only single frequency audio alert tone capability, it is recommended that the audio alert tone be in the low frequency range below 2 kHz. The CMSAAC further recommends, subject to mobile device capabilities, that the signal have a temporal pattern (on-off pattern) to make it easier to detect, particularly in noisy conditions and by people with hearing loss. See Section 7 for additional information.

Some studies show that an audio attention signal starting with a lower intensity and going to a higher intensity during the tone sequence may effectively get attention while endeavoring to avoid unduly startling the message recipient. Some mobile devices may support this capability; however, such a capability is controlled by the subscriber preferences for audio attention signal settings; this capability is not applicable to all mobile devices and should be implemented at the discretion of the mobile device vendors.

5.5.2.2 Message Content

The CMSAAC makes the following recommendations regarding message content:

General guideline: alert initiator use clear and simple language whenever possible, with minimal use of abbreviations. The most important information should be presented first.

Text messages: Follow General guideline

Audio messages: Follow General guideline. The alert initiator must insure abbreviations are spoken as full words.

Video messages: Follow General guideline.

Multimedia messages: The alert initiator should provide ample text and audio to explain images such as maps, so that message recipients understand the content of the graphics/images.

5.5.2.3 Output Mode/Display

The CMSAAC makes the following recommendations regarding output mode/display:

General guideline: The mobile device should provide an easy way to allow the user to recall the message for review.

Outside the scope of CMSAAC are alternate delivery mechanisms that would enable a CMAS-registered person to sign up with a third party for alternate format message delivery. This would provide the means to access speech delivery for people who do not have text-to-speech (TTS) functionality in their phones, and would enable delivery of American Sign Language (ASL) if available and supported by the user's handset and service. The CMSAAC recommends that the Alert Aggregator have the capability to deliver alerts to third party services in order for them to deliver accessible alerts to users with special needs.

The need to support languages other than English is recognized. See Section 5.7 Multi-Language CMAS Alert Recommendations for further information.

Text Messages:

The mobile devices should use a font to make the message easily readable. Per the American Foundation for the Blind, the goal in font selection is to use easily recognizable characters, either standard Roman or Sans Serif fonts. Another good choice is Arial. Avoid decorative fonts.

The use of color should be avoided for the purpose of conveying information, as some people are color-blind, and some devices do not display color.

If technically feasible, the mobile device display should provide high contrast display and provide adjustable font size.

One area of particular concern is that people who are blind or visually impaired will be most underserved by a solely text-based CMAM. The Committee recognizes that these subscribers could be best served by having the CMAM made available in speech format. There are mobile devices and software on the market with screen reading and text-to-speech conversion capability. It is agreed that such specialized mobile devices, which are geared for people who are blind and who have low vision, could be a solution.[7] The CMSAAC recommends that participating CMSPs who elect to transmit CMAS alert messages strongly consider offering this capability.

In mobile devices/software that includes capabilities to support text-to-speech access, the CMAS text should be accessible to the screen-reading functions in phones that are capable of generating text- to-speech. The opt-out menus on displays also should be available to these screen readers. The CMSAAC recommends that the CMAS text is accessible to these screen readers when CMAS capability is incorporated in those devices.

Future Audio Alert Message:

Follow the general guideline. Alert initiators should insure that speech is enunciated and presented at a slow pace. Alert initiators should provide a text version along with the audio version. Note this is not the text-based alert; this is a multimedia alert that contains both a text and audio component consistent with the multimedia profiles.

Future Video Alert Message:

Follow the general guideline. Alert initiators should provide text versions of the audio content of video alerts. CMSPs and mobile device vendors should consider appropriate methods for delivery and allowing users the ability to display this associated text on mobile devices as technology evolves and video and captioning capabilities become available. Also, the alert initiator should provide an audio description of the video content as a separate multimedia audio component consistent with the multimedia profiles.

Future Multimedia Alert Message:

Follow the general guideline. The alert initiator should provide all information in text and graphical form as part of the multimedia components to the alert message. The alert initiator should provide an audio description of the important information supplied in the graphic, which is a separate multimedia component consistent with the multimedia profiles.

5.5.2.4 Behavior on Receipt of a Message

It is desirable to have the CMAM prominently presented on the mobile device without user interaction when the alert message is received. To turn off the notification of the CMAS message, a familiar command consistent with the other commands used for message handling on the mobile device is recommended. It is best to avoid requiring the subscribers to remember and use a unique command or command sequence. The need to scroll or manipulate the device should be minimized.

5.5.2.5 CMAS-Related Print and Online Materials

As important to the accessibility of the CMAS is the accessibility of any CMAS-related consumer information in print or electronic form. Providing information that incorporates accessibility solutions for individuals with special needs may also bring benefits to the general population, not just users with disabilities, as studies of multimodal learning have shown. Listed here are a variety of available resources

[7] For more information, the American Foundation for the Blind (AFB) is an authoritative resource for accessible devices and related technology developments:
http://www.afb.org

that present solutions to accessibility obstacles in formats designed to easily educate and assist publishers. The Web Accessibility Initiative (WAI) develops strategies, guidelines, and resources to help make the Web accessible to people with disabilities. The following WAI resources are intended to provide basic information for people who are new to Web accessibility. The *W3C – World Wide Web Consortium (W3C) Web Content Accessibility Guidelines* are available at http://www.w3.org/WAI/

The principles of universal design — designing to meet the needs of as many users as possible — provide a new dimension for improving the usability of electronic materials for everyone. The Carl and Ruth Shapiro Family National Center for Accessible Media at WGBH developed *Accessible Digital Media Design Guidelines for Electronic Publications, Multimedia and the Web*, available at http://ncam.wgbh.org/publications/adm/

The above resources are provided for informational purposes to ensure the accessibility of all CMAS related print and web content. It is not the intent of the CMSAAC to make recommendations for existing web content or web content not associated with CMAS.

For future multimedia capabilities, if web content is delivered to the mobile device, consideration should be given to the proposed World Wide Web Consortium (W3C) Mobile Web Best Practices 1.0.

5.5.3 Subscriber CMA Opt-Out Recommendations

As stated in the WARN Act, the Commercial Mobile Alert (CMA) subscriber opt out process may be supported by a Commercial Mobile Service Provider (CMSP) that elects to transmit.

- Opt-out is defined in Section 602.(b).(2).(E) in the WARN Act as "the capability of preventing the subscriber's device from receiving such alerts, or classes of such alerts, other than an alert issued by the President"
- "Receiving such alerts" may also be interpreted to "notify and display to the user of such alerts" as the mobile device may actually receive the alert but not present it to the subscriber

As noted in Section 5.1, there are three classes of Commercial Mobile Alert Service (CMAS) Message categories:

4. Presidential-level
5. Imminent threat to life and property
6. Child Abduction Emergency or "AMBER Alert"

Presidential-level messages must always be transmitted and are not eligible for the opt-out procedure. Imminent Threat alerts are messages where the CAP severity field is Extreme or Severe, the CAP urgency field is Immediate or Expected, and the CAP certainty field is Observed or Likely. AMBER Alert messages are considered a different message classification and are treated separately..

The CMSAAC recommends that CMSPs shall offer their subscribers a simple opt-out process that is based on the classification of imminent threat and AMBER Alerts. Except for presidential messages, which are always transmitted, the process should allow the choice to opt-out of:

- All messages[8],
- All severe messages*[9],
- AMBER Alerts[10]

[8] Presidential messages will still be received

[9] Extreme messages, AMBER Alerts and presidential messages will still be received (Extreme messages are those messages where the CAP severity field is Extreme, the CAP urgency field is Immediate, and the CAP certainty field is Observed or Likely).

[10] All other messages will still be received.

* Severe messages are those messages where the CAP severity field is Severe, the CAP urgency field is Expected, and the CAP certainty field is Likely.

Because of differences in the way CMSPs and device manufacturers provision their menus and user interfaces, CMSPs and device manufacturers shall have flexibility on how to present the opt-out choices to subscribers.

5.6 Recommendations for CMAM Transmissions

The CMSAAC recommends that the CMAM be retransmitted into an effected area until the alert expires. This will provide the alert to those that might have missed the initial broadcast alert, e.g., been in the process of a voice call, those that might have had their mobile device turned off when the alert was issued or those that might be entering the area after the alert was issued.

The interval and frequency of transmission of CMAM performed by the CMSP is based upon balancing the capabilities of the CMSP specified delivery technology and various factors, such as:

- Number of simultaneous active alerts
- Number of languages
- Mobile device battery life
- Latency from alert initiator to receipt by first mobile device
- Notification to subscribers entering alert area
- Limitations of delivery technology
- Configuration of delivery technology and mobile devices
- Impact to normal call processing.

Therefore, the CMSAAC recommends that the CMSP determine the frequency of retransmissions based upon the considerations and optimization of the above mentioned factors.

5.7 Multi-Language CMAS Alerts Recommendations

The WARN Act requires the CMSAAC to submit to the Commission recommendations ‘for the technical capability to transmit emergency alerts by electing commercial mobile providers to subscribers in languages in addition to English, to the extent practical and feasible.” {Sec. 603(c)(4)}.

The CMSAAC has analyzed the technical feasibility of supporting multilanguage CMAS alerts on the various delivery technologies and has determined that support of languages other than English is a very complex issue. Fundamentally the existing air interfaces of commercial mobile service providers have technical limitations and the support of multiple languages may result in a significant impact to capacity and latency due to these limitations.

In addition, an important question is how many languages should be considered? On a National basis, only Spanish exceeds 1% of households. On a local basis, however, there are potentially more than 37 languages that exceed 1% of households which would require more than 16 different character sets to be supported in the mobile device. This raises issues such as character set limitations, the amount of CMAS alert message traffic that would need to be delivered in multi-languages, bandwidth limitations, increased cost and complexity, mobile device capabilities and deployment impacts. Additional character sets to support multiple languages also will potentially limit the amount of data that can be transmitted; for example, some character sets require 2 Bytes per character versus 1 Byte per character, and thus 90 characters available in the text profile for a CMAM now reduces the text message to 45 characters. Additional languages increase the cost and complexity both in the mobile device and in the CMSP network. At the present time, the

CMSAAC believes there are fundamental technical problems to reliably implement any languages in addition to English.

Provision has been made in the CMAS architecture to support language extensions, for example the C interface contains fields to identify language and character encoding (see Section 10.4). Such extensions are reserved for a time at which the engineering impact of additional language sets is understood.

It is recognized that there is a strong desire for the CMAS to support Spanish in addition to English. A CMSP may choose to transmit alerts received in languages other than English based on the capabilities of the technology the CMSP has deployed to support CMAS alerts, the capabilities of the mobile device, the CMSP's policy, and the definition of the the single unified Federal policy for the support of alerts in multiple languages. In addition, the Alert Gateway would need to be able to generate CMAM in multiple languages.

The CMSAAC recommends that CMSPs not be required to give notification in its election to transmit alerts, at point of sale or through any other means, or to the CMSP's subscriber base for not supporting the transmission in languages other than English.

A fundamental requirement for the optional support of languages other than English is that the CMAM must be delivered to the Commercial Mobile Service Provider in the language that it is to be delivered and in the CMAS format. At the current time, there shall be no language translation in the CMSP network or in the mobile device. This requirement should be reviewed as technology improvements are developed.

5.8 CMAS Reception Control on Mobile Devices

CMAS reception control is required where subscribers and/or CMSPs should be allowed to control the reception of CMAS alerts via control of the delivery technology (e.g., broadcast) on a CMAS-capable mobile device. The CMSAAC recognizes the WARN Act requirements of not being able to opt-out of Presidential messages. However, the primary justifications for allowing a subscriber and/or CMSP to control the CMAS delivery technology capabilities on the mobile devices include:

a. Providing the ability of not presenting CMAS alert messages to users that may not understand or may experience undue alarm such as parents wanting to suppress this service for young children or the elderly.

b. Disabling the broadcast capability when traveling to locations where the CMAS services are not desired or not supported and thus preserving battery life in normal circumstances.

c. In the presence of the CMSP radio signal, potential savings on battery life, which may be critical in an emergency or disaster situation especially where power is not available to recharge the mobile device.

d. Disabling the broadcast capability for mobile devices that are being used for special applications where the CMAS service is not applicable such as a backup notification method for in-home security systems.

e. Being able to disable the broadcast capability for CMSPs that elect not to transmit alerts in whole or in part.

Based upon the above, the CMSAAC recommends:

1. The CMSP will have the capability to enable or disable the broadcast capabilities or CMAS functionality on any of their associated mobile devices. This capability is under CMSP control mechanisms such as mobile device provisioning, and the CMSP shall be required to give notification to the subscribers as defined in Section 3.4.

2. The mobile device user may have the capability on their mobile device to disable the delivery technology for the CMAS alert messages. The execution of this capability by the subscriber shall

require confirmation of the action by the subscriber and there are no additional CMSP notification requirements as described in Section 3.4.

5.9 Roaming

The CMSAAC recommends that roaming be supported only on an intra-technology basis. For example:

1. Roaming GSM subscribers receive CMAS alerts from GSM operators in the serving market.

2. Roaming CDMA subscribers receive CMAS alerts from CDMA operators in the serving market.

3. If a Commercial Mobile Service Provider elects not to support CMAS alerts, subscribers from other Commercial Mobile Service Providers will not receive CMAS alert messages when roaming onto that Commercial Mobile Service Provider's network.

4. If a Commercial Mobile Service Provider elects not to support CMAS alerts and subscribers from that Commercial Mobile Service Provider roam onto another Commercial Mobile Service Provider network which does support CMAS alerts, that roaming subscriber will receive CMAS alert messages only if their mobile device is configured to receive CMAS alert messages with the delivery technology of roamed-to Commercial Mobile Service Provider network.

5. Inbound roamers may be supported if the mobile device is configured for, is eligible to receive and is technically capable of receiving CMAS alert messages with the delivery technology of the serving Commercial Mobile Service Provider network.

6 Service Profiles

The CMAS architecture and recommendations are based upon the principles of service profiles. Commercial mobile operators may utilize any broadcast technology to the mobile devices which comply with the service profiles. The following service profiles are defined

- Text Profile
- Streaming Audio Profile (future capability)
- Streaming Video Profile (future capability)
- Downloaded Multimedia Profile (future capability)

The CMSAAC recommends that each CMAS alert sent to the CMSP Gateway contain, at a minimum, the attributes for the text profile. Optionally, there may be multiple streaming audio, streaming video, and/or downloaded multimedia attributes associated with the CMAS alert sent to the CMSP Gateway.

Specifically, the following will be the service profiles associated with a CMAS alert sent to the CMSP Gateway:

- One Text Profile
- Zero or more Streaming Audio Profiles
- Zero or more Streaming Video Profiles
- Zero or more Downloaded Multimedia Profiles

The following section provides general recommendations and conclusions on text, audio, video, and multimedia resources.

6.1 Conclusions on Text, Audio, Video & Multimedia Resources

1. The CMSAAC recommends that the formats for future streaming audio, streaming video, and multimedia be defined at point where implementation and deployment of these technologies have reached a point where a standard set of formats can be identified, e.g., at the initial biennial review described in Section **Error! Reference source not found.**. The CMSAAC also recommends that the alert initiation systems do not implement any coding formats for these types of resources until the full impact to the end-to-end CMAS system is understood.

2. The CMAS service profiles for text, audio, video, and multimedia messages are for the transmission of text data, audio files, video files, and multimedia files and not for the presentation of real-time content.

3. The Commercial Mobile Service Provider networks are outside the scope of the trust model of the government alerting infrastructure.

4. The Alert Gateway is responsible for collecting and assembling all text, audio, video, and multimedia components of the CMAS messages to be given to the Commercial Mobile Service Providers for transmission.

a. If the CAP message includes a Resource Element that includes an URI, it is not expected that the Commercial Mobile Service Providers will be required to retrieve the file specified by the URI. Rather, the Alert Gateway will retrieve the associated file during the collection and assembly process for the CMAS alert message for retrieval by the Commercial Mobile Service Providers.

b. Any audio, video, and multimedia files collected for the CMAS alert messages must be provided to the Commercial Mobile Service Providers in a standard set of formats.

5. The CMSAAC recommends that the government alerting infrastructure be aligned with the capabilities and requirements as defined under the CMAS.

a. The above referenced initial CMAS service profiles are not capable of providing real-time multimedia broadcasts including a Presidential audio alert.

6.2 Text Profile

Support of the text profile is the minimum requirement for any Commercial Mobile Service Provider which elects to support CMAS.

This information is passed from the Alert Gateway to the CMSP Gateway and may include attributes that are generated by the CMAS alert originator.

Table 6-1 Text Profile

Service Profile: Text_Universal_Service_Profile		
Attribute Name	**Attribute Definition**	**Note**
Purpose	Common denominator for text messages	
Maximum Payload Size	120 bytes	Size is estimated
Maximum Displayable Message Size	90 characters for an English language CMA encoded with 7-bit encoding	Languages other than English, or coding other then 7-bit coding, will result in a change to the maximum number of characters supported
Data Coding Scheme	UTF-8 as defined in IETF RFC-3629	The text on the C interface is provided in UTF-8 format which is capable of supporting text in English and other languages. It is the responsibility of the CMSP Gateway to translate to any character format encoding required by the CMSP selected delivery technology.

6.3 Streaming Audio Profile (future capability)

The streaming audio profile defines the attributes for the support of streaming audio based CMAS alerts. Support of the streaming audio profile is optional for any Commercial Mobile Service Provider which elects to support CMAS and is dependent on the technology selected by the Commercial Mobile Service Provider and mobile device capabilities.

This information is passed from the Alert Gateway to the CMSP Gateway and may include attributes that are generated by the CMAS alert originator.

Table 6-2 Streaming Audio Profile

SERVICE PROFILE: STREAMING_AUDIO_SERVICE_PROFILE		
ATTRIBUTE NAME	ATTRIBUTE DEFINITION	NOTE
PURPOSE	**DEFINE SERVICE PROFILE FOR STREAMING AUDIO MESSAGES**	
MAXIMUM SIZE	**BASED UPON THE AUTHORIZED GOVERNMENT ENTITY POLICY**	**SIZE OF THE STREAMING AUDIO FILE IS DEPENDENT ON THE FILE TYPE AND ENCODING ALGORITHMS.** **SIZE OF CMAS ALERTS WITH STREAMING AUDIO COMPONENTS ARE MUCH LARGER THAN TEXT BASED CMAS ALERTS AND, THEREFORE, COULD HAVE GREATER IMPACT TO BANDWIDTH REQUIREMENTS, MESSAGE LATENCY, ETC.**
C INTERFACE DATA CODING SCHEME	**IDENTIFICATION OF THE STANDARD FORMAT OF THE STREAMING AUDIO FILE BEING RETRIEVED BY THE CMSP GATEWAY**	**SEE REFERENCE MODEL**
C INTERFACE AUDIO FILE REFERENCE	**ISSUE OF AUDIO FILE TRANSMISSIONS REMAINS TO BE ADDRESSED.**	**THE CONTENTS OF THIS ATTRIBUTE ARE BASED UPON THE STREAMING AUDIO FILE BEING PULLED BY THE CMSP GATEWAY FROM THE ALERT GATEWAY.**

6.4 Streaming Video Profile (future capability)

The streaming video profile defines the attributes for the support of streaming video based CMAS alerts. Support of the streaming video profile is optional for any Commercial Mobile Service Provider which elects to support CMAS and is dependent on the technology selected by the Commercial Mobile Service Provider and mobile device capabilities.

This information is passed from the Alert Gateway to the CMSP Gateway and may include attributes that are generated by the CMAS alert originator.

Table 6-3 Video Profile

Service Profile: Streaming_Video_Service_Profile		
Attribute Name	**Attribute Definition**	**Note**
Purpose	Define service profile for streaming video alert messages	
Maximum Size	Based upon the authorized government entity policy	Size of the streaming video file is dependent on the file type and encoding algorithms. Size of CMAS alerts with streaming video components are much larger than text based CMAS alert messages and, therefore, could have greater impact to bandwidth requirements, message latency, etc.
C Interface Data Coding Scheme	Identification of the standard format of the streaming video file being retrieved by the CMSP Gateway	See reference model
C Interface Video File Reference	Issue of video file transmissions remains to be addressed.	The contents of this attribute are based upon the streaming video file being pulled by the CMSP Gateway from the Alert Gateway.

6.5 Downloaded Multimedia Profile (future capability)

The downloaded multimedia profile defines the attributes for the support of CMAS alerts with multimedia files (e.g., graphics, photos, maps, animation) which are to be downloaded to the mobile device. Support of the downloaded multimedia profile is optional for any Commercial Mobile Service Provider which elects to support CMAS and is dependent on the technology selected by the Commercial Mobile Service Provider and mobile device capabilities. The multimedia files for download to the mobile device are distributed using broadcast mechanisms instead of point-to-point mechanisms based upon by the Commercial Mobile Service Provider selected technology.

This information is passed from the Alert Gateway to the CMSP Gateway and may include attributes that are generated by the CMAS alert originator.

Table 6-4 Downloaded Multimedia Profile

Service Profile: Downloaded_Multimedia_Service_Profile		
Attribute Name	**Attribute Definition**	**Note**
Purpose	Define service profile for CMAS alerts with multimedia files for download to the mobile device.	
Maximum Size	Based upon the authorized government entity policy	Size of the multimedia file for downloaded is dependent on the file type and encoding algorithms. Size of CMAS alerts with multimedia components for download to the mobile device are much larger than text based CMAS alert messages and, therefore, could have greater impact to bandwidth requirements, message latency, etc.
C Interface Data Coding Scheme	Identification of the standard format of the multimedia file being retrieved by the CMSP Gateway	See reference model
C Interface Multimedia File Reference	Issue of multimedia file transmissions remains to be addressed.	The contents of this attribute are based upon the multimedia file being pulled by the CMSP Gateway from the Alert Gateway.

7 Mobile Device Functionality for CMAS Alerts

This section describes the impact to the mobile devices for the support of CMAS alerts and organized into the following topics:

- General Requirements on Mobile Device Functionality
- Mobile Device Audio Attention Signal & Vibration Cadence Recommendations
- CMAS Functionality on Mobile Device
- Impact to Mobile Device Battery Life

7.1 General Requirements on Mobile Device Functionality

The CMSAAC recommends that the commercial mobile service provider and the mobile device vendors have the flexibility in the design and implementation of mobile devices in order to take the maximum advantages of advances in mobile device technologies and to account for the evolution of mobile devices and the capabilities of the future. The CMSAAC further recommends that:

1. Mobile device behavior is outside the scope of the WARN Act and, therefore, is not subject to recommendations by the CMSAAC.

2. There be a common audio attention signal and a common vibration alert cadence for CMAM. (See Section 7.2)

3. The functionality and features of the mobile device after the receipt of the CMAM (e.g., message storage, message expiration, alert presentation visual interface and user acknowledgement to the mobile device of alert messages) will be commercial mobile service provider and mobile device specific.

4. Legacy deployed mobile devices may not be supported. At a minimum, new CMAS functionality is needed on future mobile devices.

    a. New mobile devices will be introduced by normal market mobile device lifecycle replacement.

    b. Some legacy pager devices may be able to be updated with over the air programming

5. Distribution of the CMAS alert messages to the Commercial Mobile Service Provider's subscribers will be unidirectional from the Commercial Mobile Service Provider network to the mobile device of the subscriber. There will not be any acknowledgement or confirmation of receipt from the mobile device.

6. CAP messages will not be delivered to mobile devices of the subscribers.

7.2 Mobile Device Audio Attention Signal & Vibration Cadence Recommendations

Currently most Americans are familiar with the current EAS audio attention signals on radios and televisions which have been in use since the 1960s. Reproduction of this audio attention signal on mobile devices is the most recognizable method to notify the American public of CMAS alert message.

The EAS uses a two tone system for audio alerts which is a combination of 853Hz and 960Hz sine waves. For devices capable of supporting dual tone EAS audio attention signals, the CMAS audio attention signal

should sound as close to the EAS audio attention signals as can be feasibility achieved with the capabilities of the mobile devices.

The single tone for the NOAA warning alarm tone for NOAA Weather Radios and commercial broadcast stations is 1050Hz. EAS audio attention signals on commercial broadcast stations are 8 to 25 seconds in duration and the NOAA warning alarm tone is 8 to 10 seconds.

The CMSAAC recommends that temporal patterns of the CMAS audio attention signal should be supported if technologically feasible. The recommended temporal pattern of the CMAS audio attention signal is one long tone of approximately 2 seconds followed two short tones of approximately 1 second each with approximately ½ second gap between tones. The entire sequence is repeated twice with approximately ½ second between repetitions. Temporal patterns of the CMAS audio attention signal are mobile device manufacturer specific.

For devices that have polyphonic capabilities, the CMSAAC recommends that the audio attention signal consist of the two EAS tones. For devices which have only single frequency alert tone capability, it is recommended that the CMAS audio attention signal be in the low frequency range below 2 kHz.

The CMSAAC recommends that the vibration cadence for the CMAS alert signal be noticeably different from the default cadence of the mobile device and should be similar to the temporal pattern of the audio attention signal and is mobile device manufacturer specific.

If both CMAS audio and vibration cadence alerts are available, the two modes do not need to be activated simultaneously but will follow the user's settings in the mobile device; if the mobile device supports dual activation the signals will be simultaneous according to user settings, but otherwise will be separate signals.

The CMSAAC recommends that neither the CMAS audio attention signal nor the vibration cadence provided by the CMSP for the CMAS alert should be selectable by the subscriber for any mobile device functions. However, the CMSAAC acknowledges that there is no way to prevent the subscriber from downloading a ring tone that emulates the CMAS audio attention signal.

The CMSAAC recommended that the CMAS audio attention signal and the associated vibration cadence shall not be used for any application other than CMAS. The CMSAAC further recommended that the CMAS audio attention signal and the associated vibration cadence should be protected via copyright and/or trademarks and should be available for appropriate use on free and non-discriminatory basis.

7.3 CMAS Functionality on Mobile Device

This section contains the CMSAAC's conclusions and recommendations regarding the CMAS functionality on the mobile device that is needed to support CMAS alerts.

1. If the end user has muted the mobile device audio and alarms, the CMAS audio attention signal will not be activated upon receipt of a CMAS alert.
2. If the end user has deselected or turned off the vibration capabilities of the mobile device, the special emergency alert vibration cadence will not be activated upon receipt of a CMAS alert.
3. If the end user has both muted the mobile device audio and alarms and has deselected or turned off the vibration capabilities of the mobile device, neither the CMAS audio attention signal nor the special emergency alert vibration cadence will be activated upon receipt of a CMAS alert.
4. Subject to the limitations of the CMSP selected broadcast technologies and the mobile devices, the presentation of the received CMAS alert message should take priority over other mobile device functions except for the preemption of an active voice or data session.
5. If the end user does not acknowledge the CMAS alert to the mobile device, the mobile device should support the capability to activate and deactivate the CMAS audio attention signal and/or should

activate and deactivate the special emergency alert vibration cadence, if mobile device has vibration capabilities. The frequency and interval of the activation and deactivation of the CMAS audio attention signal and/or the special emergency alert vibration cadence is dependent on Commercial Mobile Service Provider policies and mobile device capabilities.

6. In order to minimize the possibility of network congestion and false alerts, mobile devices should not support any user interface capabilities to forward received CMAS alerts, to reply to received CMAS alerts, or to copy and paste CMAS alert contents.

7. The presentation of CMAS alert messages to the subscriber on the mobile device should be distinguishable from any other types of textual messages received by the mobile device subject to mobile device capabilities.

    a. Color cannot be a required method for distinguishing CMAS alert messages from other types of text messages on the mobile device since all mobile devices do not have color display capabilities.

    b. Color cannot be used as the sole method for convening information. (See Section 5.5)

7.4 Impact to Mobile Device Battery Life

The CMSAAC recommends that government Alert Aggregator support a policy of ensuring that the aggregate CMAM rate does not adversely impact mobile device battery life.

The CMSAAC recommends that the CMSPs give consideration to modifications to network infrastructure, mobile devices and/or standards, and to the proper selection of the criteria below, in order to limit the reduction of battery life.

This analysis was limited in scope to text based messages, and does not analyze the impacts of other profiles, such as audio, video or multimedia. The delta impact on portable device battery life of text based alert messages of CMAS depends upon the following input criteria:

a) Delivery Technology (GSM, UMTS, CDMA2000 1x, Flex, Re-Flex, etc.)

b) Initial system network parameters before implementation of broadcast messaging

c) Maximum latency to deliver the message over the E interface

d) Retransmission interval

e) Number of languages supported

f) Number of alerts sent

g) Alert Duration, and number of times the portable device alerts the user

Each technology implements text broadcast messaging differently. In addition, each technology is deployed with different hardware and software, as well as, different standards releases. During the battery life evaluation, these issues explain the wide range of reported battery life impact of text Broadcast Messaging. The battery life impact of CMAS on a state of the art deployment of infrastructure and portable devices targeting optimized battery life could be as high as 40% or more.

When using older technology or different network parameters, the impact to battery life can be quoted as a lower percentage. Although, the battery life will be lower than the optimized solution with cell broadcast enabled.

Although there are limitations in today's implementation of Cell Broadcast, it can be utilized for transmission of Emergency Alerts. The impact to portable device battery life can be managed through careful selection of the above parameters. The high impact parameters influenced by the CMSAAC are

maximum latency to deliver the message over the E interface, Retransmission interval, Number of languages supported, Number of alerts sent, and Alert Duration.

With modifications to network infrastructure, mobile devices and/or standards, and proper selection of the above criteria, the reduction of battery life can be less than 10% of today's capability for monitoring the Cell Broadcast channel without sending alerts messages. These modifications could potentially adversely the timeline given in Section **Error! Reference source not found.**. When alert messages are sent, e.g. a disaster situation with multiple alerts sent from multiple agencies, the reduction of battery life increases proportionally to the number of messages sent and can approach up to 40% of the battery life.

To design and deploy a system with the performance described above, modifications to the portable devices, network infrastructure and/or standards are required. These changes are scheduled in the proposed timeline for deployment of CMAS.

8 Security for CMAS Alerts

8.1 Alert Interface & Aggregator Trust Model

8.1.1 Trust Model Definitions

The following definitions are offered for clarity and specificity.

- Identity – A trusted agent will verify the identity of each individual that will be requesting credentials.
- Responsibility – The individual will have the duties of issuing public alerts and warnings on behalf of their respective jurisdiction.
- Jurisdiction – The area a person has authority to send public alert and warning messages
- Authority – Any public servant that is permitted by their jurisdiction to send a public alert and warning message.
- Capability – The nominated individual must demonstrate the knowledge of process, content and policy pertaining to the issuance of public alerts and warnings. The minimum requirement shall be a national level computer based training course. States and or local jurisdictions may require further training if they so desire.
- Credential – A specified form of evidence that an individual has completed the verification of identity, responsibility and capability. This credential will allow the individual to send or countersign a public alert and warning message.
- Certified system – will support the trust model and counter-signatory function to send public alert and warning messages.
- Countersigned – A public alert and warning message must be digitally signed by two credentialed personnel for acceptance into the CMAS.
- Originator – Can be a Federal, State, Tribal, or local jurisdiction.

8.1.2 Trust Model Requirements

The CMSAAC makes the following recommendations regarding trust model requirements:

1. All messages will be attributed reliably to an individual sender.
2. All messages will be accepted from individuals holding a specified credential or from a certified system which required individual credentials.
3. All messages must be countersigned by a second credentialed sender. All messages not countersigned will be rejected and not be sent. The sender must be notified if the message was rejected for this reason.
4. The CMSAAC recommends that a process be established by which credentials can be certified upon demonstration of identity, responsibility and capability as defined Section 12.1.1.
5. Identity, responsibility and capability must be recertified annually. All credentials will expire in 12 months.
6. All messages entered into the system will be logged, this log will be maintained for a reasonable period of time to support an audit.

7. The digital signatures will be bound to the message and carried from the originator to the Alert Gateway.

8. The message transport layer from the originator to the Alert Gateway will utilize an existing open non-proprietary transport standard and shall be Internet Protocol based.

8.2 Alert Gateway Security Requirements

The CMSAAC recommends that the Alert Gateway be protected against the potential for misuse such as hoax emergency alerts, illegal distribution of offensive content, Denial of Service (DoS/DDoS) attacks and SPAM. The CMSAAC recommends the following requirements to achieve the necessary level of security:

1. The Alert Gateway will be subject to and administered in a manner consistent with the Trust Model and shall be in compliance with Federal Information Processing Standard (FIPS) 199 and FIPS 200. The Alert Gateway shall also be in compliance with security requirements for National Critical Infrastructure/Key Resources.

2. The Alert Gateway will be part of the government alert distribution network. The interface between the Alert Aggregator and the Alert Gateway shall support the Trust Model specified in Section 8.1. The C interface is outside the scope of the Trust Model and therefore the Alert Gateway shall support standardized authentication and authorization mechanisms to interface with the CMSP Gateways.

3. A single authorized source such as a designated government agency, or their authorized agent, will serve as the sole operator for the Alert Gateway.

4. The Alert Gateway will authenticate the source of all alert transactions. If the source cannot be authenticated, the message will not be sent and a warning issued to the Alert Gateway's monitoring system.

5. The Alert Gateway will inform the alert originator via Alert Aggregator if the CMAS message was not accepted by the CMSP Gateway.

8.3 Reference Point C Security

The CMSAAC recommends that the Reference Point C interface be IP based. Therefore the security of the Reference Point C interface should be based upon standard IP security mechanisms such as VPN tunnels and IPSEC functionality.

8.4 Reference Points D & E Security

The CMSAAC recommends that the security of the Reference Points D and E be based upon CMSP policies and upon the capabilities of the CMSP selected delivery technologies.

9 CMAS Reliability & Performance

The CMSAAC recommends that, to the extent feasible, prior to the September 2008 CMSP Election, the statistical data on peak and average alert traffic volume at least for the period October 2007 thru August 2008 be available to CMSPs to support the engineering considerations for the CMSP Gateway and air interfaces. This statistical data needs to be available at the geo-targeted areas defined in section **Error! Reference source not found.** .

9.1 Alert Gateway Performance Requirements

See Annex A – Anticipated Peak & Average CMAS Traffic Volume for anticipated peak & average CMAS traffic volume. The CMSAAC makes the following recommendations regarding Alert Gateway performance requirements:

1. Based on available historical data presented to the committee, and then applying a 2X factor, it is estimated that no more than 25,000 alert messages per year will be delivered to the Alert Gateway for transmission to the various CMSPs. It is also assumed that peak rates as high as 12,000 alert messages per month and 6,000 alert messages per day are possible. For a given hour, it is also conceivable that there can be an alert for every county in the U.S. and therefore the Alert Gateway should be capable of receiving and processing 3,000 alert messages per hour and a peak rate of 30 alert messages per second.

2. The Alert Gateway will have capabilities to monitor the system utilization for capacity planning purposes and it shall be scalable to accommodate the need for additional capacity.

3. The Alert Gateway will provide a transmission control mechanism to buffer the CMAM traffic upon receiving an overload warning from the CMSP Gateway.

4. The Alert Gateway will provide the capability for a CMSP or CMSP Gateway to temporarily disable the transmission of all CMAMs to the CMSP Gateway. While CMAM delivery to CMSP Gateway has been stopped, the Alert Gateway shall establish an alert queue for the specific CMSP Gateway.

    a. The CMSP Gateway will notify the Alert Gateway to stop sending CMAM using an error response as described in Section 10.4.6. Once the error condition has cleared, the CMSP Gateway will notify the Alert Gateway to restart CMAM delivery and retry delivery of CMAMs in the queue if the CMAMs have not expired..

    b. The authorized government entity which manages the Alert Gateway will establish a process where an authorized CMSP representative can provide notification of a planned or unplanned outage of a CMSP Gateway and during that outage period, CMAMs are not delivered from the Alert Gateway to that specific CMSP Gateway. During a planned or unplanned outage, the ability to support test message across the Reference Point C interface will be supported as defined in section 10.4. .

5. If the CMAM delivered over the Reference Point C interface was rejected by a CMSP Gateway due to congestion or temporary transient error conditions, the Alert Gateway will establish an alert queue for the specific CMSP Gateway and retry delivering it to the CMSP Gateway by a configurable interval, e.g. every 30 seconds, if the CMAM has not expired.

6. There are two logical queues per CMSP Gateway, one logical queue for Presidential alerts and another logical queue for all other CMAMs. The processing of the Presidential queue takes priority over the non-Presidential queue.

7. If an alert queue exists for a CMSP Gateway, all incoming alerts shall be placed into the queue based upon the time the CMAM was received by the Alert Gateway.

8. The Alert Gateway will support separate alert queues for each CMSP Gateway so that queuing for one or more CMSP Gateway shall not affect alerts delivery to all other CMSP Gateways.

9. The Alert Gateway will be designed to have the service availability of 99.999%.

10. System performance will be monitored in real-time 24 hours a day seven days a week to ensure all levels of service are met and/or exceeded.

9.2 Alert Delivery Latency

The CMSAAC recommends that, since latency will require experience in deployment, end-to-end latency requirements be addressed in the biennial review.

The CMSAAC recognizes the importance of delivering CMAMs as quickly as possible from the alert initiators to the transmission within the alert area. The CMSAAC also recognizes that there are operational characteristics of the CMSP Infrastructure which impact CMAM delivery latency. These operational characteristics include the following factors:

- Mobile device battery life impact
- Call processing impact
- Capabilities of the delivery technology
- Message queues
- Number of languages
- Number of targeted cell sites / paging transceivers for the alert area
- Geo-targeting processing

It is difficult to predict or model systems that have not been designed, built, or deployed.

9.3 CMAS End-to-End Reliability

The CMSAAC recommends that the CMAS system reliability from alert initiation to the transmission of the CMAM over the CMSP selected delivery technology meet telecom standards for highly reliable systems.

In order to achieve, a feasible and practical level of CMAS reliability on an end-to-end basis:

- The Commercial Mobile Service Providers will process CMAS alerts on a best effort
- The CMAS alert message may be retransmitted according to CMSP policies and the capabilities of the CMSP selected delivery technology.

Even though many components and elements of the end to end CMAS solution have high reliability, the over-all reliability of CMAS is unpredictable for the following reasons:

- RF transmissions can be subject to noise and other interference or environmental factors
- The capabilities of the cellular environment are not predictable especially in a disaster environment. For example, it can not be predicted which and how many cell sites will remain operational after a disaster.
- The subscriber may currently be in a location that does not have any RF signal.

- The subscriber's mobile device may not have any remaining power.

9.4 Message Logging

The CMSAAC recommends that the logs on the Alert Gateway be used to identify messages received by or rejected by the CMSP Gateway. These logs will be accessible by the alert originators and by the CMSPs. These logs will be the only required audit methods for the determination of which CMAS messages were sent to the CMSPs.

The CMSAAC further recommends that, upon receipt of an alert, the CMSP Gateway will respond back to the Alert Gateway with an acknowledgment that the alert message was received or rejected. Message logging on the CMSP Gateway is a function of the system performance part of the Commercial Mobile Service Provider's business, and will not be an audit trail.

The CMSAAC recommends that there be no requirements for the CMSP to retain logs for any period of time.

9.4.1 Alert Gateway Logging

The CMSAAC makes the following recommendations regarding Alert Gateway logging:

1. The Alert Gateway will maintain a log of messages with time-stamps that verify when messages are received from the Alert Aggregator and when the messages are acknowledged or rejected by the CMSP Gateway. The log for rejected messages will include error codes for rejection as specified in Section 10.4.6.
2. The Alert Gateway will maintain an online log of active and cancelled alert messages for 90 days.
3. The Alert Gateway will maintain archived logs for a minimum of 36 months.
4. The Alert Gateway will provide CMSPs access to online messaging logs and archived logs for testing and trouble shooting purposes.
5. The Alert Gateway will generate monthly system and performance statistics reports based on CMA alerting category, alerting originator, alerting area and other alerting attributes.
6. The Alert Gateway will provide the capability for a CMSP to temporarily disable the transmission of all CMAMs to the CMSP Gateway. This event will be captured in the log file. Cancellation of the event should be noted in the log file as well.

9.5 CMAS Testing

End-to-end testing of the CMAS is defined to be testing from the Alert Initiator to the CMSP Gateway. This testing will verify the A, B, and C reference points, as well as the function of the Alert Aggregator, Alert Gateway, and CMSP Gateway. It is undesirable to send test messages over the CMSP infrastructure to the mobile devices as these messages could cause considerable confusion to the end user, as well as utilizing CMSP network resources.

Using real event codes for testing purposes poses the risk of unintentionally alarming and confusing recipients. For this reason, and to insure that a test message does not propagate to the CMSP subscriber base, the CMSAAC recommends that all end-to-end testing be indicated using the CAP *status* element with a value of "test", which shall be mapped to a test message over reference point C. Upon receipt of a test message, the CMSP Gateway will respond with an acknowledgment of receipt of the message and log receipt of the message according to CMSP policy.

The CMSAAC recommends that the CMSP Gateway support receiving a test message from the Alert Gateway for testing reference point C. This test message shall not be delivered to the CMSP Infrastructure nor broadcast to subscribers.

The CMSAAC recommends that the CMSP Gateway support the receipt and processing of Alert Gateway keep-alive test messages periodically. The frequency shall be configurable based on policy to be determined by the authorized government entity and the CMSPs.

The CMSAAC recommends that the keep-alive test messages *not* be sent if there are real messages to be sent.

9.5.1 General CMAS Testing Recommendations

An important part of a successful Commercial Mobile Alerting System will be the ability to effectively test and troubleshoot the various components and interfaces.

The CMSAAC recommends that this test and troubleshooting capability be integrated into the architecture and protocol of the CMA System up front, to maximize effectiveness.

The CMSAAC recommends the following primary aspects of CMAS Testing and Troubleshooting capability to allow thorough testing and troubleshooting of the end-to-end CMAS without wearying the public:

1. Provision for testing of the CMAS, including the delivery mechanisms, without requiring all subscribers to see a test message.

    a. This might be accomplished by providing signaling in the application layer which indicates a test message – which would not be displayed by 'normal terminals', but could be displayed by 'test terminals'. CMSPs could configure which devices were 'test terminals'.

    b. Provide the ability to send test messages to a single CMSP/network without impact to other CMSPs.

    c. Provide the ability to test the CMAS up to the CMSP Gateway without impacting the CMSP infrastructure.

2. Provide CMSP access to the CMAM logs from the Alert Gateway.

3. Messages used for testing purposes shall be clearly differented from messages for actual events

9.5.2 Alert Gateway Testing

The CMSAAC recommends that the Alert Gateway support several types of testing:

a. Functional testing for the C interface (not expected to be sent to the subscribers)

b. Connection testing for new CMSP

The CMSAAC further recommends the following requirements for Alert Gateway testing:

1. The Alert Gateway will support initiating a test message for each service profile implemented for reference point C upon request by a particular CMSP. The test message will only be sent to a specific CMSP Gateway. The message will not be broadcast to subscribers.

2. The Alert Gateway will support initiating a test message for each service profile implemented for reference point C for all CMSP Gateways. The message will not be broadcast to subscribers.

3. The Alert Gateway will support keep-alive test messages periodically over the C interface. The frequency will be configurable based on policy to be determined by the authorized government entity and the CMSPs. The keep-alive test messages will not be sent if there are real messages to be sent.

4. All test messages for the C interface will be clearly marked and identified as test messages.

10 Interface Protocols for CMAS Alerts

The following two interfaces are applicable for the support of CMAS alerts in the Commercial Mobile Service Provider networks:

- Alert Gateway – Commercial Mobile Service Provider Interface which is Reference Point C
- Commercial Mobile Service Provider – Mobile Device Interface for CMAS alert content which is Reference Point D

Both of these interfaces are defined in this section.

10.1 Reference Point A Protocol

The CMSAAC recommends that reference Point A interface requirements consist of the following:

1. The message sent to the Alert Aggregator must consist of one of the following:
    a. A valid CAP 1.1 message with all mandatory elements.
        - Message ID
        - Sender ID
        - Sent Date/Time
        - Message Status
        - Message Type
        - Scope
        - Event Category
        - Urgency
        - Severity
        - Certainty
        - Resource description
        - Area Description – A FIPS geo-code, a polygon or circle (WGS-84 format) will be used to support the area description.
2. The Alert Gateway will provide a mechanism to validate the identity of the individual sending the message to allow non-repudiation.
3. The implementer of the alert aggregator will provide a documented, non-proprietary, specification for transport that will support appropriate security and reliability.

10.2 Reference Point B Protocol

The CMSAAC recommends that reference Point B interface requirements consist of the following:

1. The implementer of the Alert Gateway will provide a documented non-proprietary specification for the B interface which will support appropriate security and reliability.

10.3 Alert Gateway Interfaces & Mapping Requirements

10.3.1 Alert Gateway Interface Requirements

The CMSAAC recommends the following requirements for the Alert Gateway interfaces:

1. The Alert Gateway will support an open, non-proprietary interface to the Alert Aggregator (e.g. IP).
2. The Alert Gateway will initially support CAP v1.1 as the application layer protocol for communicating with the Alert Aggregator.
3. The Alert Gateway will uniquely identify each CMSP Gateway identified by a unique IP address or domain name.
4. The Alert Gateway will support the "C" interface protocol as defined in Section 10.4.
5. The Alert Gateway will support all CMAM formats that can be delivered to CMSP Gateway.
6. The Alert Gateway will support the common service profile formats as referred to in Section 6 for text, audio, video and multimedia transmission of alert messages to the CMSP Gateways.
7. The Alert Gateway will support receiving acknowledgement from the CMSP Gateway that the CMAM has been received or rejected by the CMSP Gateway.
8. If any mandatory parameter/attribute is not included in the CAP message sent over the B interface, the Alert Gateway will use a default parameter value if available, or reject the CAP message if a default parameter value is not available.

10.3.2 Alert Gateway Interface Mapping Requirements

The Alert Gateway will map the CMAMs received in CAP format into the CMAC format supported by the CMSP Gateway.

1. If eventCode = "EAN", the CMAM will be handled as a Presidential Alert. The Alert Gateway will not forward messages with eventCode = "EAT" or "NIC" to the CMSP Gateway.
2. The Alert Gateway will deliver CMAMs using the same language as issued by the alert originator and will not do language translation as a gateway function.
3. Each CMAM will only include one language. The CMA issued in multiple languages will be issued by separate messages.
4. All CMAM alert, update & cancellation messages will come only from the alert originators, including Presidential alert. The Alert Gateway will pass these messages to the CMSP Gateway. The Alert Gateway is not required to generate alerts, alert updates and/or cancellations.
5. The Alert Gateway will not alter the content of text alert messages, with the exception of
    a. If CAP expires is not available, the default parameter value of one hour shall be used.
    b. Constructing the text alert message using CAP elements such as category, eventCode and responseType. The algorithm for constructing the text alert message is described in Section 5.3.
6. For Presidential Alert, the Alert Gateway will use the following CAP elements to construct the message:

a. Use CAP parameter (with valueName = CMAMtext), if available and less than the maximum CMA message length limit. If not, then

b. Use Alert Gateway generated automatic text: "The President has issued an emergency alert. Check local media for more details."

7. For AMBER Alert, the Alert Gateway will use the following CAP elements to construct the message:

a. Use CAP parameter (with valueName = CMAMtext), if available and less than the maximum CMA message length limit. If not, the Alert Gateway will reject the message.

8. For alerts other than the Presidential Alert or AMBER Alert, the Alert Gateway will support free-format text generation or automatic text generation.

9. For free-format text generation, the Alert Gateway will use the CAP parameter (with valueName = CMAMtext) to construct the message. If the CAP parameter (with valueName = CMAMtext) is not available or exceeds the maximum CMA message length limit, the Alert Gateway will reject the message.

10. For automatic text generation, the Alert Gateway will support the following rules to construct the message:

a. What's happening: The Alert Gateway will use the expanded text as defined in Table 3.1 for the CAP eventCode element if available. If eventCode is not provided, the Alert Gateway will use the expanded text as defined in Table 3.1 for the CAP category element.

b. Recommended action: The Alert Gateway will use the CAP responseType element if available. If responseType is not provided, the Alert Gateway will not include this information.

c. Area Affected: The Alert Gateway will use the phrase "in this area".

d. Expiration time with time zone: The Alert Gateway will translate the time according to Table 3.1 for the CAP expires element if provided. The Alert Gateway will use the time zone provided in the CAP expires element or may use the time zone in the affected area. If not provided, the Alert Gateway will use one hour from the current time as a default. If the affected area has more than one time zones, the Alert Gateway will use one of the time zones.

e. Sending Agency: The Alert Gateway will translate it according to Table 3.1 for the CAP sender element. The translated sending agency should not exceed the maximum length of 12 characters in order to fit into the maximum CMA message length limit. The translated sending agency will be truncated to 12 characters if it causes the constructed message to exceed the maximum CMA message length limit.

11. If the CAP message received by the Alert Gateway is not formatted correctly, the Gateway will reject the message and inform the Alert Originator.

12. If a CAP message contains multiple INFO blocks with the same headline but different area elements, the Alert Gateway will collapse it into a single CMAM with a single INFO block and multiple area elements before sending it to the CMSP Gateway.

13. If a CAP message contains multiple INFO blocks with the different headlines, the Alert Gateway will create separate CMAM with each INFO block. The Alert Gateway will process the INFO blocks in the order contained in the CAP message.

14. The Alert Gateway will not do translations of the character sets.

15. The Geo-mapping of targeted area (cell sites) will be the responsibility of CMSPs and not a function of the Alert Gateway.

16. The Alert Gateway will provide the geo-targeting information over Reference Point C in accordance with the CMSP profile stored within the Alert Gateway.

17. The Alert Gateway will provide Geocode as specified in Section 10.4 to the CMSP Gateway..

18. The Alert Gateway will translate latitude/longitude coordinates into appropriate State or County Geocode if no State or County Geocode is provided by alert originator.

19. The Alert Gateway will not be required to translate State or County Geocode into latitude/longitude coordinates.

20. The Alert Gateway will specify an agreed upon maximum number of latitude/longitude coordinates per polygon to be sent to the CMSP Gateway.

21. If Geocode, polygon or circle is not provided for a Presidential alert, the Alert Gateway will use "Nation wide" by default.

22. If Geocode, polygon or circle is not provided for any non-presidential alert or update, the Alert Gateway will reject the message and return an error to the alert originator.

23. For audio, video and multi-media CMAMs, if the CAP message includes the associated files, the Alert Gateway will

    a. Re-format, if necessary, the associated files into standardized format as specified in the associated service profile (see Section 6).

    b. Store the associated files on the Alert Gateway to be retrieved by the CMSP Gateways.

    c. Send the message with proper URL so that CMSP Gateways can retrieve the files if they so choose.

24. For audio, video and multi-media CMAMs, if the CAP message includes only the URL but not the associated files, the Alert Gateway will

    a. Retrieve the associated files from the URL in the CAP message

    b. Re-format, if necessary, the associated files into standardized format as specified in the associated service profile (see Section 6).

    c. Store the associated files on the Alert Gateway to be retrieved by the CMSP Gateway.

    d. Send the message with proper URL so that CMSP Gateway can retrieve the files if they so choose.

25. The Alert Gateway, via Reference Point C, will always provide the Commercial Mobile Service Provider Gateway, the CMAC_geocode as defined in Section 10.4. Additionally, if available, the Alert Gateway will provide one or more of the following parameters to identify the alert area: CMAC_polygon, CMAC_circle or CMAC_gnis format..

26. The Alert Gateway will be responsible to generate the CMAC geocode(s) corresponding to the alert area from the CAP "area" element. The CMAC geocode(s) corresponding to the alert area will be

generated from either the area described by the polygon or circle, conversion of the SAME code or ZIP code for the alert area, or using the FIPS value if specified in the original CAP alert message.

27. If the original CAP message does not contain a polygon, circle, or geocode, the Alert Gateway will reject the message unless the message originator was the President, in which case the alert area will be assumed Nationwide in the absence of the area information.

28. CAP will be the protocol used on the "B" interface to carry the CMAM into the Alert Gateway. Not all the elements and values allowed by CAP are useful for CMAMs. Also some elements are optional in CAP but required by CMAMs. The Alert Gateway will apply the following mapping and filtering rules for all the messages received via the "B" interface as shown in Table x.x. The following is a description of the column shown in Table x.x.x:

    Column 1: Lists the CAP element.

    Column 2: Lists the code values applicable to CMAMs.

    Column 3: Lists the filtering and mapping rules to be used by the Alert Gateway. "Passing" means the element and code value will be passed from the "B" interface to the "C" interface. "Mapping" means the CAP element and code value will be mapped into the appropriate CMAC attribute. "Rejecting" means the Alert Gateway will reject the CAP message received from the "B" interface and no message will be sent over the "C" interface. "Ignoring" means the CAP element is not applicable to CMAM and will be ignored by the Alert Gateway. "Generating" means the Alert Gateway will generate the appropriate CMAC elements and attributes.

    Column 4: Lists the corresponding "C" interface CMAC elements as defined in Section 10.4

Table 10-1 Parameter mapping from "B" Interface CAP message in to "C" Interface CMAC message

CAP Element	(CMA) Permitted Values	Alert Gateway Filtering Rules	CMAC Element
N/A		Generating by the Alert Gateway	CMAC protocol version
N/A		Generating by the Alert Gateway	CMAC sending Alert Gateway id
alert	N/A	Ignoring	N/A
identifier (free format)		Mapping from the free format into a 2 octets hex number	CMAC_message_identifier (2 octets hex number)
sender		Passing	CMAC_sender
sent		Mapping into UTC format	CMAC_sent_date_time
status	"Actual" "Exercise" "System" "Test"	Passing with permitted values; Rejecting message with "Draft"	CMAC_status
msgType	"Alert" "Update" "Cancel" "Error"	Passing with permitted values; Rejecting message with "Ack"	CMAC_message_type

source	N/A	Ignoring	
scope	"Public"	Reject message if "Public" is not in field.	N/A
restriction		Rejecting message if this element is included	N/A
addresses		Rejecting message if this element is included	N/A
code		Ignoring	N/A
note		Passing	CMAC_cancel_error_node
references		Mapping from the free format into a 2 octets hex number	CMAC_referenced_message_identifier (2-octet hex number)
incidents	N/A	Ignoring	N/A
N/A		Generating by the Alert Gateway	CMAC_original_cap_alert_uri
info		Ignoring	
language		Passing	CMAC_text_language
category		Mapping	CMAC_category
event	N/A	Ignoring	N/A
responseType	All but "Assess"	Reject message with "Assess" in field, pass all others	CMAC_response_type
urgency	"Immediate" "Expected"	Passing with permitted values or rejecting message with other values	CMAC_urgency
severity	"Extreme" "Severe"	Passing with permitted values or rejecting message with other values	CMAC_severity
certainty	"Observed" "Likely"	Passing with permitted values or rejecting message with other values	CMAC_certainty
audience	N/A	Ignoring	N/A
eventCode	"EAN" "CAE"	Mapping "EAN" to "Presidential"; Mapping "CAE" to "Child Abduction"; Mapping other values to "No special handling"	CMAC_special_handling
eventCode		Mapping	CMAC_event_code
effective	N/A	Ignoring	N/A
onset	N/A	Ignoring	N/A
expires		Passing; Rejecting message if already expired; Applying default value of one hour if not provided	CMAC_expires_date_time
senderName		Mapping	CMAC_sender_name

headline		Conditional passing when eventCode= “EAN” or “CAE”; Ignoring when eventCode has other values.	CMAC_text_alert_message
description	N/A	Conditional passing when eventCode= “EAN”, Ignoring when eventCode has other values.	CMAC_text_alert_message
N/A	ASCII 7-bit	Generating by the Alert Gateway	CMAC_text_encoding
N/A	Less than 90 characters	Generating by the Alert Gateway	CMAC_text_message_length
N/A		Generating by the Alert Gateway as specified in Section 5.5	CMAC_text_alert_message
instruction	N/A	Ignoring	N/A
web		Mapping to a local link on the Alert Gateway	CMAC_web_link
contact	N/A	Ignoring	N/A
parameter	N/A	Conditional passing when eventCode= “EAN” or “CAE”; Conditional passing when eventCode has other values and parameter valueName = “CMAMtext”; Ignoring otherwise	CMAC_text_alert_message
resource	N/A	Ignoring	N/A
resourceDesc		Mapping	CMAC_resource_description
mimeType		Mapping	CMAC_mime_type
size		Mapping	CMAC_resource_size
uri		Mapping to a local link on the Alert Gateway	CMAC_uri
derefUri	N/A	Ignoring	N/A
degest		Ignoring	
area	N/A	Ignoring	N/A
areaDesc		Passing	CMAC_area_description
polygon		Passing	CMAC_polygon
circle		Passing	CMAC_circle
geocode		Passing, or generating based on polygon and/or circle	CMAC_cmas_geocode
geocode		Generating based on polygon and/or circle	CMAC_cmas_gnis
altitude	N/A	Ignoring	N/A
ceiling	N/A	Ignoring	N/A

1

29. If an incoming CAP message fails the Alert Gateway validation or filtering rules, an error message will be sent over the "B" interface to the alert originator. The error message may contain additional information in the "note" element. The "note" element in the error response to the alert originator may contain multiple error messages. The following are some examples of error responses.

    a. CMA error #1: Unsupported code value of "<value> " in element "<element name>" (e.g. scope="Private")

    b. CMA error #2: Missing required element "<element name>" (e.g. element Y = eventCode)

    c. CMA error #3: Unsupported element "<element name>" (e.g. element Z = restriction)

    d. CMA error #4: Text message length exceeds maximum limit

10.4 Reference Point C Protocol

The C reference point is the interface from the Alert Gateway to the CMSP Gateway. The C reference point is used to map the CAP elements into the CMSP protocol on the C reference point ("CMAC"), as follows:

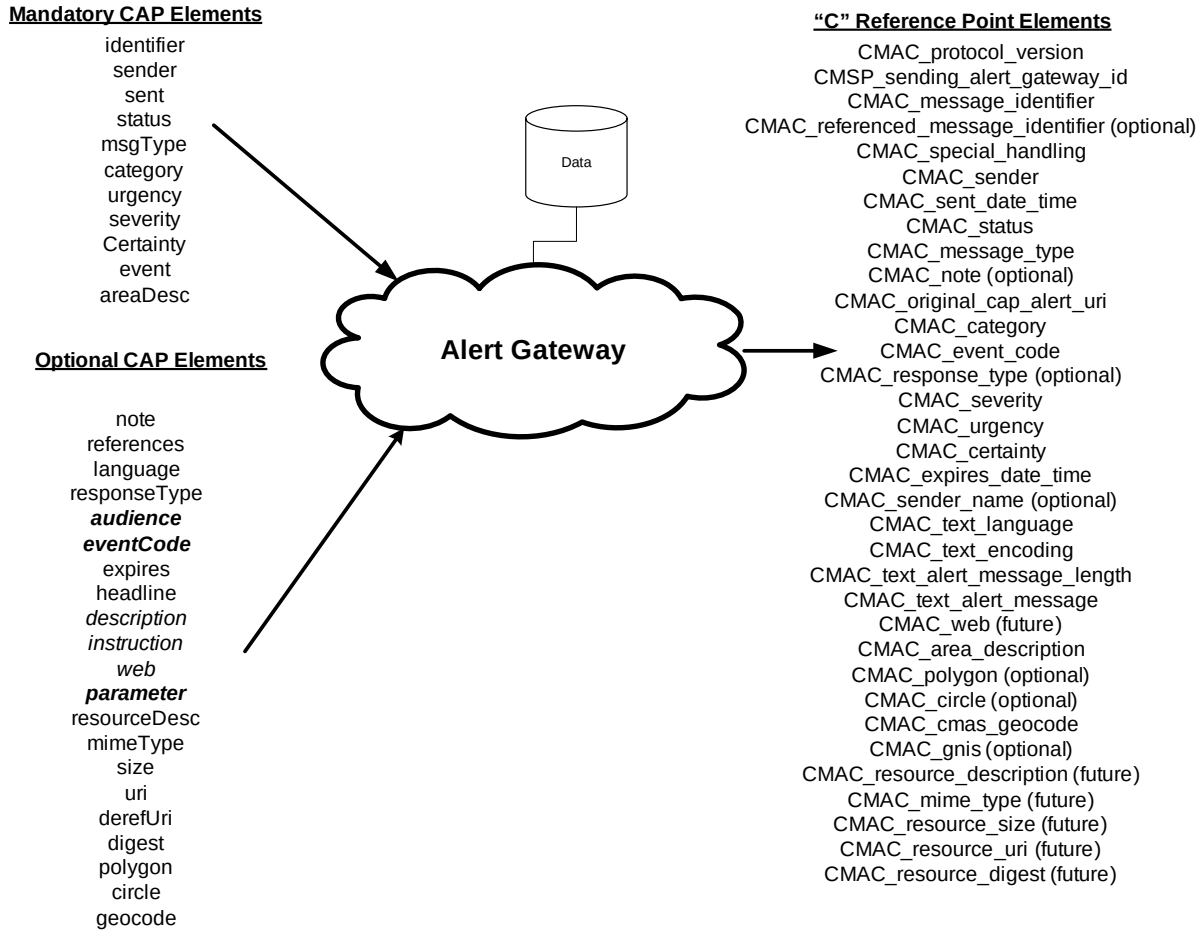

Figure 10-1 Relationship of CAP Elements to Reference Point C Elements

10.4.1 Structure of the CMA "C" Reference Point Protocol

The CMSAAC recommends that each CMAC Alert message consist of the following segments:

- CMAC Alert Attributes segment
- CMAC Alert Info segment
- CMAC Alert Area segment
- CMAC Alert Resource segment

The CMSAAC recommends that the CMAC Alert Message document object model be as follows:

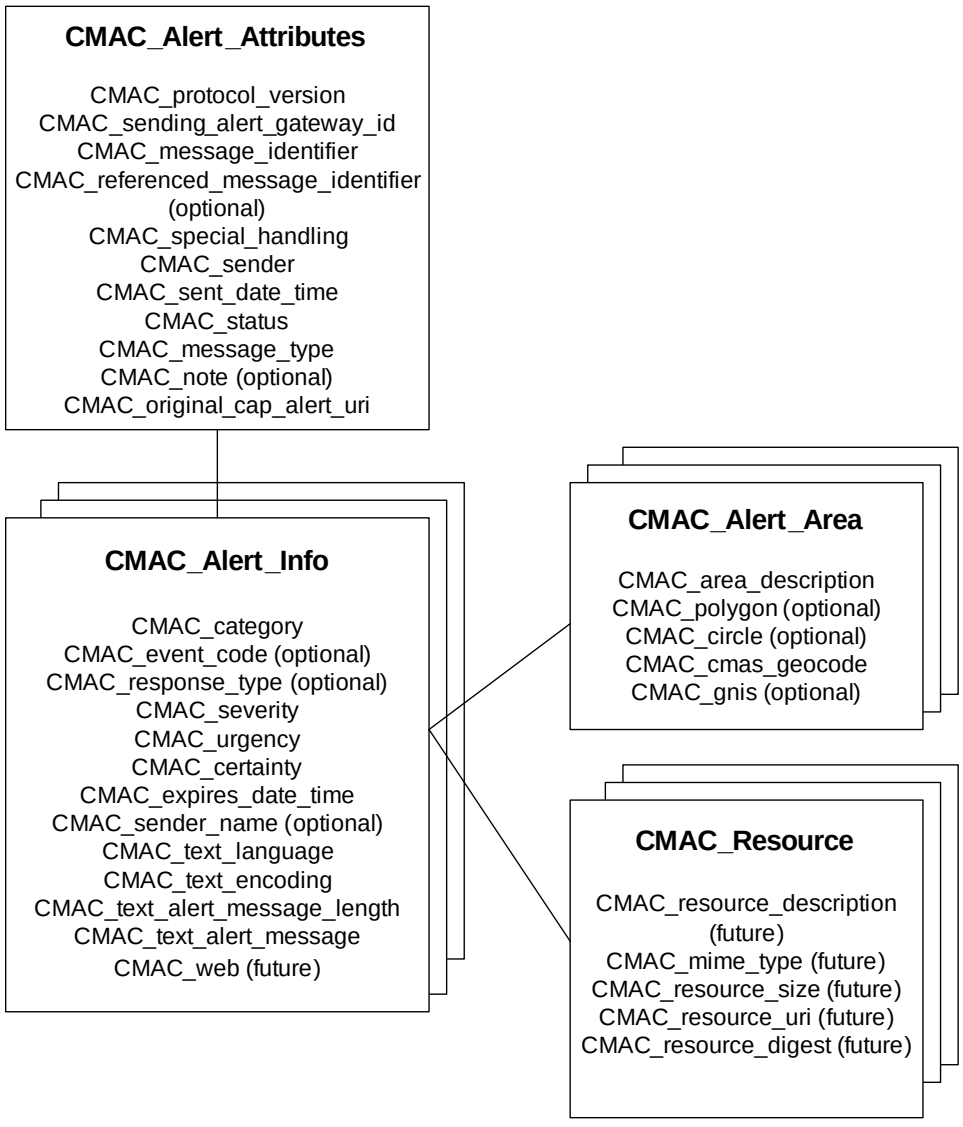

Figure 10-2 CMAC Message Structure

The CMSAAC recommends that a CMAC Alert Message must contain:

- one CMAC_Alert_Attributes segment
- one or more CMAC_Alert_Info segments
- one or more CMAC_Alert_Area segements.

The CMAC_Resource segment is optional for future use in streaming audio, streaming video, and multimedia CMAs.

10.4.2 CMAC Data Dictionary

10.4.2.1 CMAC_Alert_Attributes Segment

Table 10-2 CMAC_Alert_Attributes Segment

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_alert	M	(1) Surrounds CMAC alert message subelements. (2) MUST include the xmlns attribute referencing the CMAC URN as the namespace, e.g.: <cmac:CMAC_alert xmlns:cmac="urn:xxx:xxxxx:xx:cmac:1.0"> [sub-elements] </cmac:CMAC_alert> (3) In addition to the specified subelements, MAY contain one or more <CMAC_alert_info> blocks.
CMAC_protocol_version	M	The version of the CMAC protocol. Used by the CMSP Gateway only. Specified by the Alert Gateway.
CMAC_sending_alert_gateway_id	M	URI of the Alert Gateway sending the CMAC message. Specified by thet Alert Gateway.
CMAC_message_identifier	M	A 2-octet binary value uniquely identifying this message, assigned by the Alert Gateway and derived from the CAP identifier element. This element is sent to the mobile device.
CMAC_referenced_message_identifier	C	A 2-octet binary value uniquely identifying a referenced CMAM, assigned by the Alert Gateway. Required for an Update, Cancel or Ack CMAC_message_type. Derived from the CAP references element.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_special_handling	O	Specifies if this alert message requires special handling. Specified by the Alert Gateway, derived from CAP elements. Code Values: "**Presidential**" "**Child Abduction**" "**No Special Handling**"
CMAC_sender	M	Identifies the originator of this alert. Used by the CMSP for logging purposes only. Alert Gateway uses the CAP sender element to populate this element.
CMAC_sent_date_time	M	The date and time the message is sent by originator in UTC in XML dateTime format. Derived from the CAP sent element.
CMAC_status	M	Alert Gateway uses the CAP status element to populate this element. Code Values: "**Actual**" - Actionable by all targeted recipients "**Exercise**"- Actionable only by designated exercise participants, for CMSP use. "**System**" - For messages that support alert network internal functions. In addition this is used for the "keep alive" message between the Alert Gateway and the CMSP Gateway. "**Test**" - Technical testing of the C Reference Point only, for CMSP Gateway use only.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_message_type	M	Alert Gateway uses the CAP msgType element to populate this element. Code Values: "**Alert**" - Initial information requiring attention by targeted recipients "**Update**" - Updates and supercedes the earlier message(s) identified in < CMAC_referenced_ message_identifier > "**Cancel**" - Cancels the earlier message(s) identified in < CMAC_ referenced_ message_ identifier > "**Ack**" - Acknowledges receipt and acceptance of the message(s) identified in < CMAC_referenced_ message_ identifier > additional explanation may appear in <CMAC_note> "**Error**" indicates rejection of the message(s) identified in < CMAC_referenced_ message_ identifier >; explanation SHOULD appear in <CMAC_note>
CMAC_note	O	Optional element. Used for CMSP logging purposes for a cancel or error message type, or to provide a response back to the Alert Gateway. Alert Gateway uses the CAP note element to populate this element on messages from the Alert Gateway to the CMSP Gateway. The CMSP Gateway uses this element on messages to the Alert Gateway.
CMAC_original_cap_alert_uri	M	This element contains the uri where the CMSP may retrieve the original complete CAP version of the alert from the Alert Gateway. Specified by the Alert Gateway.

10.4.2.2 CMAC_Alert_Info Segment

Multiple occurrences are permitted within the CAP from the alert originator; the CMSAAC recommends that each occurrence be a separate CMAM from the Alert Gateway. The CMSAAC further recommends that each language be sent as a separate CMAM with a unique message identifier. It is anticipated that a separate CMAS_Alert_Info element with associated sub-elements will be created for the CMAMs to be given to the Commercial Mobile Service Providers for broadcast via the CMSP selected technologies consistent with the requirements and procedures defined by the CMSAAC.

Table 10-3 CMAC_Alert_Info Segment

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_alert_info		(1) Only a single occurrence is permitted within a single <CMAC_alert>. If there are multiple "info" segements in the original CAP message, the Alert Gateway shall format as separate CMAC messages each with a unique identifier. (2) In addition to the specified subelements, MAY contain one or more <CMAC_resource> blocks and/or one or more <CMAC_area> blocks.
CMAC_category	M	Alert Gateway uses the CAP category element to populate this element. Code Values used by CMSP Gateway only: "**Geo**" - Geophysical (inc. landslide) "**Met**" - Meteorological (inc. flood) "**Safety**" - General emergency and public safety "**Security**" - Law enforcement, military, homeland and local/private security "**Rescue**" - Rescue and recovery "**Fire**" - Fire suppression and rescue "**Health**" - Medical and public health "**Env**" - Pollution and other environmental "**Transport**" - Public and private transportation "**Infra**" - Utility, telecommunication, other non-transport infrastructure "**CBRNE**" – Chemical, Biological, Radiological, Nuclear or High-Yield Explosive threat or attack "**Other**" - Other events
CMAC_event_code	O	Alert Gateway uses the CAP eventCode element to populate this element. Optional element used by the CMSP Gateway only. A system-specific code for event typing, in the form: <CMAC_event_code> <CMAC_valueName>valueName</CMAC_valueName> <CMAC_value>value</CMAC_value> </CMAC_event_code> where the content of "CMAC_valueName" is a user assigned string designating the domain of the code, and the content of "value" is a string (which may represent a number) denoting the value itself (e.g., CMAC_valueName ="SAME" and value="TOR"). Values of "CMAC_valueName" that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME).

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
		The following SAME codes are supported in CMAS: o Civil Danger Warning CDW o Civil Emergency Message CEM o Evacuation Immediate EVI o Hazardous Materials Warning HMW o Law Enforcement Warning LEW o Local Area Emergency LAE o Nuclear Power Plant Warning NUW o Radiological Hazard Warning RHW o Shelter in Place Warning SPW o Avalanche Warning AVW o Blizzard Warning BZW o Child Abduction Emergency CAE o Coastal Flood Warning CFW o Dust Storm Warning DSW o Earthquake Warning EQW o Fire Warning FRW o Flash Flood Warning FFW o Flood Warning FLW o High Wind Warning HWW o Hurricane Warning HUW o Severe Thunderstorm Warning SVR o Special Marine Warning SMW o Tornado Warning TOR o Tropical Storm Warning TRW o Tsunami Warning TSW o Volcano Warning VOW o Winter Storm Warning WSW
CMAC_response_type	O	Alert Gateway uses the CAP responseType element to populate this element. Code values: "**Shelter**" – Take shelter in place "**Evacuate**" – Relocate "**Prepare**" – Make preparations "**Execute**" – Execute a pre-planned activity "**Monitor**" – Attend to information sources "**Assess**" – Evaluate the information in this message. (This value SHOULD NOT be used in public warning applications.) "**None**" – No action recommended Multiple instances MAY occur within a single <CMAC_info> block. This element is passed to the mobile device.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_severity	M	Alert Gateway uses the CAP severity element to populate this element. Code Values sent to the mobile device: "**Extreme**" - Extraordinary threat to life or property "**Severe**" - Significant threat to life or property
CMAC_urgency	M	Alert Gateway uses the CAP urgency element to populate this element. Code Values sent to the mobile device: "**Immediate**" - Responsive action SHOULD be taken immediately "**Expected**" - Responsive action SHOULD be taken soon (within next hour)
CMAC_certainty	M	Alert Gateway uses the CAP certainty element to populate this element. Code Values sent to the mobile device: "**Observed**" – Determined to have occurred or to be ongoing. "**Likely**" - Likely (probability > ~50%)
CMAC_expires_date_time	M	The expiry time of the information of the alert message for use by the CMSP Gateway. The date and time is represented in UTC [dateTime] format. Maximum duration is 24 hours. Derived from the CAP expires element.
CMAC_sender_name	O	Optional element for logging purposes at the CMSP Gateway. The human-readable name of the agency or authority issuing this alert. Alert Gateway uses the CAP senderName element to populate this element.
CMAC_text_language	M	Specifies the language of the text in the CMAC_text_alert_message, for use by the mobile device. Code Values: "**English**" "**Spanish**" "**French**" (future Canada use only) "**Other**" – for future use Specified by the Alert Gateway and derived from the CAP language element.
CMAC_text_encoding	M	Specifies the data encoding scheme of the text in the CMAC_text_alert_message, for use by the mobile device. Code Values: "**UTF-8**" Specified by the Alert Gateway.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_text_alert_message_length	M	The length, in characters, of the text in the CMAC_text_alert_message. Note the number of octets in the CMAC_text_alert_message can be derived from this parameter and the CMAC_text_encoding parameter. Specified by the Alert Gateway.
CMAC_text_alert_message	M	The text of the alert message for use by the mobile device. This field is defined by the CMAS Text Profile and may contain up to 90 English characters using a 7-bit encoding scheme. Other languages or data encoding schemes will change the number of characters supported. Specified by the Alert Gateway, which may be derived or obtained via CAP elements.
CMAC_web_link	O	Optional element for future use. The identifier of the hyperlink associating additional information with the alert message. This data must be in a domain accessible by the CMSP Gateway. Alert Gateway uses the CAP web element to populate this element.

10.4.2.3 CMAC_Area Segment:

Multiple occurrences are permitted

Table 10-4 CMAC_Area Segment

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_area	M	(1) Multiple occurrences permitted, in which case the target area for the <CMAC_alert_info> block is the union of all the included <CMAC_area> blocks. (2) MAY contain one or multiple instances of <CMAC_polygon> or <CMAC_circle>, and shall contain at least one instance of <CMAC_geocode>. If multiple <CMAC_polygon>, <CMAC_circle> or <CMAC_geocode> elements are included, the area described by this <area> is the union of those represented by the included elements.
CMAC_area_description	M	The text describing the affected area of the alert message for use by the CMSP for logging purposes only. Alert Gateway uses the CAP areaDesc element to populate this element.
CMAC_polygon	O	Optional element. The paired values of points defining a polygon that delineates the affected area of the alert message. Alert Gateway uses the CAP polygon element to populate this element.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_circle	O	Optional element. The paired values of a point and radius delineating the affected area of the alert message. Alert Gateway uses the CAP circle element to populate this element.
CMAC_cmas_geocode	M	The CMAS-defined geographic code delineating the affected area of the alert message. This is an extension to the FIPS code (see Section 10.4.5). Alert Gateway uses the CAP geocode, polygon, circle, and/or sender elements to derive this element.
CMSC_gnis	O	Optional element. This value is the geographic code delineating the affected area of the alert message using the U.S.G.S. Geographic Names Information System (GNIS) code. Derived by the Alert Gateway.

10.4.2.4 CMAC_Resource Segment:

Multiple occurrences are permitted. The CMAC_Resource segment is not used for the Text Profile but may be applicable to future streaming audio, streaming video, and multimedia alerts.

Table 10-5 CMAC_Resource Segment

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_resource	O	(1) Refers to an additional file with supplemental information related to this <CMAC_alert_info> element; e.g., an image or audio file (2) Multiple occurrences MAY occur within a single <CMAC_alert_info> block
CMAC_resource_description	O	Optional element. The human-readable text describing the content and kind, such as “map” or “photo,” of the resource file. For use by the CMSP Gateway for logging purposes only. Alert Gateway uses the CAP resourceDesc element to populate this element.
CMAC_mime_type	O	Optional element. The identifier of the MIME content type and sub-type describing the resource file. Alert Gateway uses the CAP mimeType element to populate this element.
CMAC_resource_size	O	Optional element. The integer indicating the size of the resource file. Alert Gateway uses the CAP size element to populate this element.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_resource_uri	O	Optional element. The identifier of the hyperlink for the resource file. Alert Gateway uses the CAP uri element to populate this element.
CMAC_digest	O	Optional element. The code representing the digital digest (“hash”) computed from the resource file. Calculated using the Secure Hash Algorithm (SHA-1) per [FIPS 180-2]. Alert Gateway uses the CAP digest element to populate this element.

10.4.3 Example CMAC XML Schema

```
<?xml version = "1.0" encoding = "UTF-8"?>
<schema xmlns = "http://www.w3.org/2001/XMLSchema"
    targetNamespace = "cmac:1.0"
    xmlns:cmac = "cmac:1.0"
    xmlns:xs = "http://www.w3.org/2001/XMLSchema"
    elementFormDefault = "qualified"
    attributeFormDefault = "unqualified">
  <element name = "CMAC_Alert_Attributes">
    <annotation>
      <documentation>CMAC Alert Message (version 1.0)</documentation>
    </annotation>
    <complexType>
      <sequence>
        <element name = "CMAC_protocol_version" type = "string"/>
        <element name = "CMAC_sending_alert_gateway_id” type = "anyURI"/>
        <element name = "CMAC_message_identifier" type = "string"/>
        <element name = "CMAC_referenced_message_identifier" type = "string" minOccurs = "0" />
        <element name = "CMAC_special_handling">
          <simpleType>
            <restriction base = "string">
              <enumeration value = "Presidential"/>
              <enumeration value = "Child Abduction"/>
              <enumeration value = "No Special Handling"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "CMAC_sender" type = "string"/>
        <element name = "CMAC_sent_date_time" type = "dateTime"/>
        <element name = "CMAC_status">
          <simpleType>
            <restriction base = "string">
              <enumeration value = "Actual"/>
              <enumeration value = "Exercise"/>
              <enumeration value = "System"/>
              <enumeration value = "Test"/>
            </restriction>
          </simpleType>
        </element>
```

```
        <element name = "CMAC_message_type">
          <simpleType>
            <restriction base = "string">
              <enumeration value = "Alert"/>
              <enumeration value = "Update"/>
              <enumeration value = "Cancel"/>
              <enumeration value = "Ack"/>
              <enumeration value = "Error"/>
            </restriction>
          </simpleType>
        <element name = "CMAC_note" type = "string" minOccurs = "0"/>
        <element name = "CMAC_original_cap_alert_uri" type = "anyURI"/>
      </element>
      <element name = "CMAC_alert_info" minOccurs = "0">
        <complexType>
          <sequence>
            <element name = "category" maxOccurs = "unbounded">
              <simpleType>
                <restriction base = "string">
                  <enumeration value = "Geo"/>
                  <enumeration value = "Met"/>
                  <enumeration value = "Safety"/>
                  <enumeration value = "Security"/>
                  <enumeration value = "Rescue"/>
                  <enumeration value = "Fire"/>
                  <enumeration value = "Health"/>
                  <enumeration value = "Env"/>
                  <enumeration value = "Transport"/>
                  <enumeration value = "Infra"/>
                  <enumeration value = "CBRNE"/>
                  <enumeration value = "Other"/>
                </restriction>
              </simpleType>
            </element>
            <element name = "CMAC_event_code" minOccurs = "0" maxOccurs = "unbounded">
              <complexType>
                <sequence>
                  <element ref = "cmac:valueName"/>
                  <element ref = "cmac:value"/>
                </sequence>
              </complexType>
            </element>
            <element name = "CMAC_responseType" maxOccurs = "unbounded">
              <simpleType>
                <restriction base = "string">
                  <enumeration value = "Shelter"/>
                  <enumeration value = "Evacuate"/>
                  <enumeration value = "Prepare"/>
                  <enumeration value = "Execute"/>
                  <enumeration value = "Monitor"/>
                  <enumeration value = "Assess"/>
                  <enumeration value = "None"/>
                </restriction>
              </simpleType>
            </element>
            <element name = "CMAC_severity">
              <simpleType>
```

```
                <restriction base = "string">
                  <enumeration value = "Extreme"/>
                  <enumeration value = "Severe"/>
                </restriction>
              </simpleType>
            </element>
            <element name = "CMAC_urgency">
              <simpleType>
                <restriction base = "string">
                  <enumeration value = "Immediate"/>
                  <enumeration value = "Expected"/>
                </restriction>
              </simpleType>
            </element>
            <element name = "CMAC_certainty">
              <simpleType>
                <restriction base = "string">
                  <enumeration value = "Observed"/>
                  <enumeration value = "Likely"/>
                </restriction>
              </simpleType>
            </element>
            <element name = "CMAC_expires_date_time" type = "dateTime" minOccurs = "0"/>
            <element name = "CMAC_sender_name" type = "string" minOccurs = "0"/>
            <element name = "CMAC_text_language" />
              <simpleType>
                <restriction base = "string">
                  <enumeration value = "English"/>
                  <enumeration value = "Spanish"/>
                  <enumeration value = "French"/>
                  <enumeration value = "Other"/>
                </restriction>
              </simpleType
            <element name = "CMAC_text_encoding" />
              <simpleType>
                <restriction base = "string">
                  <enumeration value = " UTF-8"/>
                </restriction>
              </simpleType
            </element>
            <element name = "CMAC_text_alert_message_length" type = "string" />
            <element name = "CMAC_text_alert_message" type = "string" />
            <element name = "CMAC_web" type = "anyURI" minOccurs = "0"/>
            <element name = "CMAC_alert_resource" minOccurs = "0" maxOccurs = "unbounded" >
            <complexType>
              <sequence>
                <element name = "CMAC_resource_desciption" type = "string"/>
                <element name = "CMAC_mime_type" type = "string" minOccurs = "0"/>
                <element name = "CMAC_resource_size" type = "integer" minOccurs = "0"/>
                <element name = "CMAC_resource_uri" type = "anyURI" minOccurs = "0"/>
                <element name = "CMAC_digest" type = "string" minOccurs = "0"/>
              </sequence>
            </complexType>
            </element>
            <element name = "area" minOccurs = "0" maxOccurs = "unbounded">
              <complexType>
                <sequence>
```

```
                    <element name = "CMAC_area_description" type = "string"/>
                    <element name = "CMAC_polygon" type = "string" minOccurs = "0" maxOccurs =
                    "unbounded"/>
                    <element name = "CMAC_circle" type = “string" minOccurs = "0" maxOccurs =
                    "unbounded"/>
                    <element name = "CMAC_cmac_geocode" type=”string” maxOccurs = "unbounded">
                    <element name = "CMAC_gnis" type = “string" minOccurs = "0" maxOccurs = "unbounded"/>
                    </element>
                  </sequence>
                </complexType>
              </element>
            </sequence>
          </complexType>
        </element>
        </sequence>
      </complexType>
    </element>
    <element name = "valueName" type = "string"/>
    <element name = "value" type = "string"/>
</schema>
```

10.4.4 Element Mapping from B Reference Point (CAP) to C Reference Point (CMAC) to E Reference Point (CMAE) Elements

Note: elements listed in **bold** are mandatory.

Table 10-6 Mapping Reference Point B Elements to Reference Point C Elements

CAP Element	CMAC Element	CMAE Element
N/A	**CMAC_protocol_version**	N/A
N/A	N/A	**CMAE_protocol_version**
N/A	**CMAC_sending_alert_gateway_id**	N/A
identifier	**CMAC_message_identifier**	**CMAE_identifier**
references	CMAC_referenced_message_identifier	N/A
N/A	CMAC_special_handling	**CMAE_alert_handling**
sender	**CMAC_sender**	N/A
sent	**CMAC_sent_date_time**	N/A
status	**CMAC_status**	N/A
msgType	**CMAC_message_type**	**CMAE_alert_type**
source	N/A	N/A
scope	N/A	N/A
restriction	N/A	N/A

CAP Element	CMAC Element	CMAE Element
code	N/A	N/A
note	CMAC_ note	N/A
incidents	N/A	N/A
N/A	**CMAC_original_cap_alert_uri**	N/A
category	**CMAC_category**	**CMAE_category**
event	N/A	N/A
eventCode	CMAC_event_code	N/A
responseType	CMAC_response_type	**CMAE_response_type**
severity	**CMAC_severity**	**CMAE_severity**
urgency	**CMAC_urgency**	**CMAE_urgency**
certainty	**CMAC_certainty**	**CMAE_certainty**
audience	N/A	N/A
effective	N/A	N/A
onset	N/A	N/A
expires	**CMAC_expires_date_time**	**CMAE_expires**
senderName	CMAC_sender_name	N/A
language	**CMAC_text_language**	**CMAE_language**
N/A	**CMAC_text_encoding**	**CMAE_char_set**
N/A	**CMAC_text_alert_message_length**	**CMAE_alert_text_length**
N/A	**CMAC_text_alert_message**	**CMAE_alert_text**
headline	N/A	N/A
description	N/A	N/A
instruction	N/A	N/A
web	CMAC_web_link	N/A
contact	N/A	N/A
parameter	N/A	N/A
areaDesc	**CMAC_area_description**	N/A
polygon	CMAC_polygon	N/A
circle	CMAC_circle	N/A
geocode	**CMAC_cmas_geocode**	N/A
geocode	CMSC_gnis	N/A
altitude	N/A	N/A
ceiling	N/A	N/A
resourceDesc	CMAC_resource_description	N/A
mimeType	CMAC_mime_type	N/A

CAP Element	CMAC Element	CMAE Element
size	CMAC_resource_size	N/A
uri	CMAC_resource_uri	N/A
derefUri	N/A	N/A
digest	CMAC_digest	N/A
N/A	N/A	CMAE_associated_multimedia_indicator
N/A	N/A	CMAE_CMSP_defined_parameter
N/A	N/A	CMAE_reserved

10.4.5 Definition of CMAC_cmas_geocode Element

The CMAC_cmas_geocode is five characters where the first two characters or digits identify the state or region and the last three digits identify the specific counties, regions, or equivalent entities. The CMSAAC recommends that the CMAC_cmas_geocode be assigned as follows:

1. The CMAC_cmas_geocode indication for a specific county will be as defined in Federal Information Processing Standard 6-4 (FIPS 6-4), titled "Counties and Equivalent Entities of the United States, Its Possessions, and Associated Areas", dated 31 August 1990.

2. The CMAC_cmas_geocode indication for an entire state will be the two digit FIPS State Numeric Code as defined in Federal Information Processing Standard 5-2 (FIPS 5-2), titled "Codes for the Identification of the States, the District of Columbia and the Outlying Areas of the United States, and Associated Areas", dated 28 May 1987 followed by three zeroes (000).

3. The CMAC_cmas_geocode indication for an entire United States including all states, the District of Columbia, possessions, and associated areas will be US000.

4. In the future, it is possible that alerts may be targeted for regions of the country (e.g., Gulf States). The more efficient and error resistant solution would be to have CMAC_cmas_geocode values for regional areas such as FEMA regions or National Weather Service (NWS) regions. The FEMA regions would be assigned values in the format of US0xx and the NWS regions would be assigned values in the format of US1xx.

The following table defines the CMAC_cmas_geocode value assignments.

Table 10-7 CMAC_cmas_geocode Assignments

CMAC_cmas geocode	Definition
00000	**Not Used**
00001 thru 99999	**For Identification of states and counties**
US000	**Entire United States**
US001	**FEMA Region 1 (Maine, Vermont, New Hampshire, Rhode Island, Massachusetts, and Connecticut)**
US002	**FEMA Region 2 (New York, New Jersey, Puerto Rico, and Virgin Islands)**

CMAC_cmas geocode	Definition
US003	**FEMA Region 3 (Delaware, District of Columbia, Maryland, Pennsylvania, Virginia, and West Virginia)**
US004	**FEMA Region 4 (Alabama, Florida, Georgia, North Carolina, South Carolina, Tennessee, Kentucky, and Mississippi)**
US005	**FEMA Region 5 (Illinois, Indiana, Michigan, Minnesota, Ohio, and Wisconsin)**
US006	**FEMA Region 6 (Arkansas, Louisiana, New Mexico, Oklahoma, and Texas)**
US007	**FEMA Region 7 (Iowa, Kansas, Missouri, and Nebraska)**
US008	**FEMA Region 8 (Colorado, Montana, North Dakota, South Dakota, and Utah)**
US009	**FEMA Region 9 (Arizona, California, Hawaii, Nevada, American Samoa, Guam, Commonwealth of the Northern Mariana Islands, Republic of the Marshall Islands, and Federated States of Micronesia)**
US010	**FEMA Region 10 (Alaska, Idaho, Oregon, and Washington)**
US011 thru US100	**Not Assigned**
US101	**National Weather Service (NWS) Central Region (Colorado, Illinois, Indiana, Iowa, Kansas, Kentucky, Michigan, Minnesota, Missouri, and Nebraska)**
US102	**National Weather Service (NWS) Eastern Region (Maine, Maryland, Massachusetts, New Jersey, New York, North Carolina, Ohio, Pennsylvania, South Carolina, and Vermont)**
US103	**National Weather Service (NWS) Southern Region (Alabama, Arkansas, Florida, Georgia, Louisiana, Mississippi, New Mexico, Oklahoma, Puerto Rico, Tennessee, and Texas)**
US104	**National Weather Service (NWS) Western Region (Arizona, California, Idaho, Montana, Nevada, Oregon, Utah, and Washington)**
US105	**National Weather Service (NWS) Alaska Region (Alaska)**
US106	**National Weather Service (NWS) Pacific Region (Hawaii, Guam, America Samoa)**
US107 thru US999	**Not Assigned**

10.4.6 Definition of CMAC Response Codes

The CMSAAC recommends the following as the response codes that may be returned from the CMSP Gateway to the Alert Gateway in the CMAC_note element in response a received CMAS message via the Reference Point C interface:

CMAC_Error_100 Invalid Alert Gateway ID

CMAC_Error_101 Unsupported protocol version
CMAC_Error_102 Segment XXX missing
CMAC_Error_103 Invalid message length
CMAC_Error_104 Mandatory element XXX missing
CMAC_Error_105 Conditional element XXX missing which is required based upon value of element YYYY
CMAC_Error_106 Optional element XXX not allowed
CMAC_Error_107 Unrecognized value in element XXX
CMAC_Error_108 Value in element XXX is out of acceptable range
CMAC_Error_109 Value XXX of element YYY not supported
CMAC_Error_110 Invalid length of element XXX
CMAC_Error_111 Expiration time greater than allowed interval
CMAC_Error_112 Failure to convert text message into alphabet encoding scheme
CMAC_Error_113 Text encoding not compatible with specified text language
CMAC_Error_114 Special handling element not consistent with message content
CMAC_Error_115 Polygon element contains more than maximum number of coordinates
CMAC_Error_200 Failure to retrieve additional alert info from Alert Gateway

CMAC_Error_201 Message received after expiration time
CMAC_Error_203 Message update failed
CMAC_Error_204 Message cancellation failed

CMAC_Error_300 Alert message failed due to insufficient system storage
CMAC_Error_301 CMSP server error
CMAC_Error_302 Maximum number of sessions reached (if C interface is session based)

CMAC_Resp_400 CMAS test successful
CMAC_Resp_401 CMAS test failed due to XXX

CMAC_Resp_500 Transient error on CMSP Gateway – Discontinue transmission of alerts
CMAC_Resp_501 Resume transmission of alerts to CMSP Gateway
CMAC_Resp_502 Keep alive message response

10.4.7 Example CMAS "C" Interface Alert Messages

As an example of a CMAS Alert Message, consider the following CAP alert message from the National Weather Service:

```
<cap:alert xmlns:cap="http://www.incident.com/cap/1.0">
        <cap:identifier>NOAA-NWS-ALERTS Arizona 2007-08-01T18:22:17-04:00</cap:identifier>
        <cap:sender>w-nws.webmaster@noaa.gov</cap:sender>
        <cap:sent>2007-08-01T18:22:17-04:00</cap:sent>
        <cap:status>Actual</cap:status>
        <cap:msgType>Alert</cap:msgType>
        <cap:scope>Public</cap:scope>
        <cap:note>Current Watches, Warnings and Advisories for Arizona Issued by the National
        Weather Service</cap:note>
        <cap:references>http://www.weather.gov/alerts/az.html</cap:references>
  <cap:info>
        <cap:category>Met</cap:category>
        <cap:event>Flash Flood Warning</cap:event>
        <cap:urgency>Expected</cap:urgency>
        <cap:severity>Severe</cap:severity>
        <cap:certainty>Likely</cap:certainty>
        <cap:effective>2007-08-01T22:11:00</cap:effective>
        <cap:expires>2007-08-01T23:15:00</cap:expires>
        <cap:headline>Flash Flood Warning</cap:headline>
        <cap:description>FLASH FLOOD WARNING AZC005-012315- BULLETIN - EAS ACTIVATION
        REQUESTED FLASH FLOOD WARNING NATIONAL WEATHER SERVICE FLAGSTAFF AZ
        311 PM MST WED AUG 1 2007 THE NATIONAL WEATHER SERVICE IN FLAGSTAFF HAS
        ISSUED A * FLASH FLOOD WARNING FOR... SOUTH CENTRAL COCONINO COUNTY IN
        NORTH CENTRAL ARIZONA... * UNTIL 415 PM MST * AT 306 PM MST...NATIONAL
        WEATHER SERVICE DOPPLER RADAR INDICATED FLASH FLOODING FROM A
        THUNDERSTORM OVER THE WARNED AREA. * LOCATIONS IN THE WARNING INCLUDE
        HIGHWAY 89 THROUGH OAK CREEK CANYON BETWEEN SLIDE ROCK STATE PARK
        AND MIDGELY BRIDGE. THE HEAVY RAINS WILL LIKELY TRIGGER LIFE-THREATENING
        ROCKSLIDES... MUDSLIDES...AND DEBRIS FLOWS NEAR THE BRINS FIRE BURN AREA
        IN OAK CREEK CANYON...AS WELL AS FLOODING OF CREEKS...ROADS...AND
        NORMALLY DRY WASHES. DO NO ATTEMPT TO DRIVE THROUGH THIS AREA UNTIL
        THE THREAT HAS DIMINISHED. LAT...LON 3488 11177 3489 11169 3499 11169 3498 11177
$$ DB</cap:description>
        <cap:web>http://www.weather.gov/alerts/AZ.html#AZC005.FGZFFWFGZ.221100</cap:web>
        <cap:area>
                <cap:areaDesc>Kaibab Plateau, Marble, Glen Canyons, Grand Canyon Country,
        Coconino Plateau, Northeast Plateaus, Mesas Hwy, Little Colorado River Valley in,
        Western Mogollon Rim, Eastern Mogollon Rim, Oak Creek, Sycamore Canyons,
        Northeast Plateaus, Mesas Sou (Arizona)</cap:areaDesc>
                <cap:geocode>004005</cap:geocode>
        </cap:area>
  </cap:info>
        </cap:alert>
```

This Alert Gateway would construct a CMAS "C" Interface message based on this CAP alert as follows:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAS_alert xmlns = "urn:xxx:xxx:xx:xxx:cmac:1.0">
   <CMAC_protocol_version>1.0</ CMAC_protocol_version >
   <CMAC_alert_gateway_id>http://cmas_alert_gateway.gov</ CMAC_alert_gateway_id >
   <CMAC_identifier>1056</identifier>
   <CMAS_sender> w-nws.webmaster@noaa.gov </CMAS_sender>
   <CMAC_sent_date_time>2003-06-17T14:57:00-07:00</CMAC_sent_date_time>
   <CMAC_status>Actual</CMACstatus>
   <CMAC_message_type>Alert</CMAC_message_type>
   <CMAC_alert_gateway_id>http://cmas_alert_gateway.gov/CMAM1056</CMAC_alert_gateway_id >
   <CMAC_alert_info>
     <CMAC_category>Met</CMAC_category>
      <CMAC_severity>Severe</CMAC_severity>
      <CMAC_urgency>Expected</CMAC_urgency>
      <CMAC_certainty>Likely</CMAC_certainty>
       <CMAC_expires_date_time>2007-08-01T23:15:00</CMAC_expires_dalt_time>
       <CMAC_text_language>English</ CMAC_text_language >
       <CMAC_text_encoding>ISO-6739-2</ CMAC_text_encoding>
       <CMAC_text_message_length>56</ CMAC_text_message_length>
       <CMAC_message>Severe Weather Warning until 4:15pm MST</ CMAC_message>
      <CMAC_area>
         <CMAC_area_description>Kaibab Plateau, Marble, Glen Canyons, Grand Canyon Country,
          Coconino Plateau, Northeast Plateaus, Mesas Hwy, Little Colorado River Valley in,
          Western Mogollon Rim, Eastern Mogollon Rim, Oak Creek, Sycamore Canyons,
          Northeast Plateaus, Mesas Sou (Arizona)</CMAC_area_description>
          <CMAC_geocode>004005</CMAC_geocode>
       </CMAC_area>
   </CMAC_alert_info>
</CMAC_alert>
```

This CMAM would be broadcast as:

Severe Weather Warning in this area until 4:15pm MST NWS

10.5 Reference Point E Protocols

The protocols that will be used for Reference Point E are dependent upon the capabilities of the delivery technology or technologies that have been selected by the CMSP.

The following is the CMA specific information that must be delivered over Reference Point "E" to support the CMAS text profile; mapping of this information to the delivery technology is beyond the scope of the CMSAAC:

Table 10-8 Reference Point E Protocol Elements

Parameter	Function
CMAE_protocol_version	CMAE protocol version
CMAE_identifier	A number uniquely identifying this message.

Parameter	Function
CMAE_alert_handling	Identifies special handling for the alert: – Presidential Alert. – Child Abduction Emergency (i.e., AMBER Alert) Additional values are reserved for future use.
CMAE_alert_type	Alert message is new, update or cancel CMAS alert
CMAE_language	Language of the alert message in the CMAE_Alert_Text parameter.
CMAE_char_set	Character set for the alert message in the CMAE_Alert_Text parameter (e.g., GSM 7-bit encoding, ISO 639-2, UCS-2, UTF-16)

1

2

11 Annex A – Anticipated Peak & Average CMAS Traffic Volume

In 2006, there was a total of 9239 tornado and flash flood warnings in the U.S. as reported by the National Weather Service. The following has a breakdown by state of these warnings:

Table 11-1 Table of Total 2006 Tornado & Flash Flood Warnings by State

STATE	TOR	FFW
AL	223	109
AR	152	142
AZ	11	292
CA	13	142
CO	54	68
CT	2	24
DC	0	10
DE	4	15
FL	106	24
GA	99	36
HI	1	163
IA	66	26
ID	24	16
IL	325	164
IN	212	175
KS	206	80
KY	152	291
LA	169	100
MA	1	11
MD	11	116
ME	4	27
MI	23	17
MN	70	46
MO	467	287
MS	300	82
MT	2	11
NC	108	171
ND	70	19
NE	67	27
NH	1	2
NJ	5	56
NM	11	167
NV	4	29
NY	14	218
OH	55	139
OK	112	34
OR	1	4
PA	22	326
SC	79	18
SD	71	24
TN	209	141
TX	382	753
UT	1	100
VA	54	362
VT	2	5
WA	0	7
WI	74	37
WV	2	64
WY	9	12
TOTAL	4050	5189

It can be assumed that these warnings account for approximately 50% of all warnings issued in 2006. In addition, there are approximately 1200 child abduction emergency/Amber Alerts per year.

Given the above statistics and adding a factor of uncertainty in, the anticipated initial yearly CMAMs for a single language of English which meet the criteria for CMAs is assumed to be 25,000 alerts per year. This number is expected to grow due to increased usage and due to the potential support of additional languages in the future.

On a monthly basis, the tornado and flash flood data is as follows:

Table 11-2 Table of 2006 Tornado & Flash Flood Warnings by State by Month

2006	Tornado	Flash Flood	Total
January	134	109	243
February	53	48	101
March	769	398	1167
April	916	238	1154
May	520	476	996
June	281	1124	1405
July	163	946	1109
August	211	703	914
September	407	530	937
October	290	370	660
November	202	186	388
December	104	61	165
Total '06	4050	5189	9239

Using these actual alert statistics as a percent of the total per month, and applying to the 25,000 estimate number yields the following estimate of alerts per month:

Table 11-3 Estimated CMA Volume by Month

CMA Estimate Per Month	
January	658
February	273
March	3158
April	3123
May	2695
June	3802
July	3001
August	2473
September	2535
October	1786
November	1050
December	446
Total	25000

Note there is significant uncertainty in these estimates as one cannot predict “mother nature” or human activities. These estimates should only serve as guidelines to the anticipated message traffic in the CMAS.

12 Annex B – WARN Act Statutory Requirements

12.1 WARN Act Requirements

1. Transmission of emergency alerts via commercial mobile service is voluntary.
    a. Commercial mobile service operators may voluntarily elect to transmit emergency alerts {Sec. 602(a)}.

2. A commercial mobile service operator who elects to transmit emergency alerts agree to do so in a manner consistent with the technical standards, protocols, procedures, and other technical requirements implemented by the Commission {Sec. 602(b)(2)(B)(ii)}.

3. A commercial mobile service operator who elects to transmit emergency alerts can elect to transmit the emergency alert services in whole or in part {Sec. 602(b)(1)(B)}.[11]

4. A commercial mobile service operator who elects in whole or in part NOT to transmit emergency alerts:
    a. Must provide clear and conspicuous notice at point-of-sale of any devices with which its commercial mobile service is included, that it will not transmit such alerts via the service it provides for the device. {Sec. 602(b)(1)(B)}
    b. Must provide notification of this decision to its existing subscribers. {Sec. 602(b)(1)(C)}
    c. Shall not by itself provide a basis for liability against the provider (including its officers, directors, employees, vendors, and agents) {Sec. 602(e)(2)}

5. Commercial mobile service licensee may not impose a separate or additional charge for such transmission or capability {Sec. 602(b)(2)(C)}

6. Any commercial mobile service licensee electing to transmit emergency alerts may offer subscribers the capability of preventing the subscriber's device from receiving such alerts, or classes of such alerts, other than an alert issued by the President. {Sec. 602.(b)(2)(E) & Sec. 603(c)(5)}

7. Commercial mobile service providers who elect to transmit emergency alerts may transmit in languages in addition to English to the extent practical and feasible. {Sec. 603(c)(4)}

8. Any commercial mobile service provider (including its officers, directors, employees, vendors, and agents) that transmits emergency alerts and meets it obligations under this title shall not be liable to any subscriber to, or user of, such person's service or equipment for
    a. Any act or omission related to or any harm resulting from the transmission of, or failure to transmit, an emergency alert. {Sec. 602(e)(1)(A)}
    b. The release to a government agency or entity, public safety, fire service, law enforcement official, emergency medical service, or emergency facility of subscriber information used in connection with delivering such an alert. {Sec. 602(e)(1)(B)}

[11] The Committee interprets the definition of "in whole or in part" to include the following: All or a subset of the mobile operator's service area and/or all or a subset of current and future mobile devices supported by the mobile operator network

12.2 WARN Act Interpretations

12.2.1 CMSP Election

The WARN Act specifies the election process for a CMSP that elects to transmit CMAs as follows:

> 602(b)(2) ELECTION-
>
> (A) IN GENERAL- Within 30 days after the Commission issues its order under paragraph (1), each licensee providing commercial mobile service shall file an election with the Commission with respect to whether or not it intends to transmit emergency alerts.

The above mentioned election process must be complete in September, 2008 as specified in the timelines in the WARN Act.

The CMAS requires new technology development and deployments, including development of mobile device functionality for CMAS and new mobile devices. The requirements for this new technology will not be available until the completion of the CMSAAC process and the completion of the FCC Report and Order in April, 2008 as specified by the WARN Act. Typical development cycles for a development of this magnitude require up to 12 months of standardization work in the appropriate standards bodies once the requirements are finalized followed by 18-24 months implementation and deployment before availability of the service and supporting mobile devices.

Thus, a CMSP that files an election with the Commission in September 2008 with the intent to transmit emergency alerts is making a commitment to support the development and deployment of technology for the following:

- "C" reference point
- CMSP Gateway
- CMSP Infrastructure
- Mobile Device with CMAS functionality and support of the CMSP selected technology

However, the technology, capabilities for deployment, and mobile devices may not be available for initial deployment and subscriber purchase potentially 12 months plus 18-24 months (approximately 30-36 months) following the CMSAAC recommendation, due to the required standardization and development cycles for the technology and capabilities of the mobile devices. Full deployments may not occur until a much later timeframe via a phased implementation.

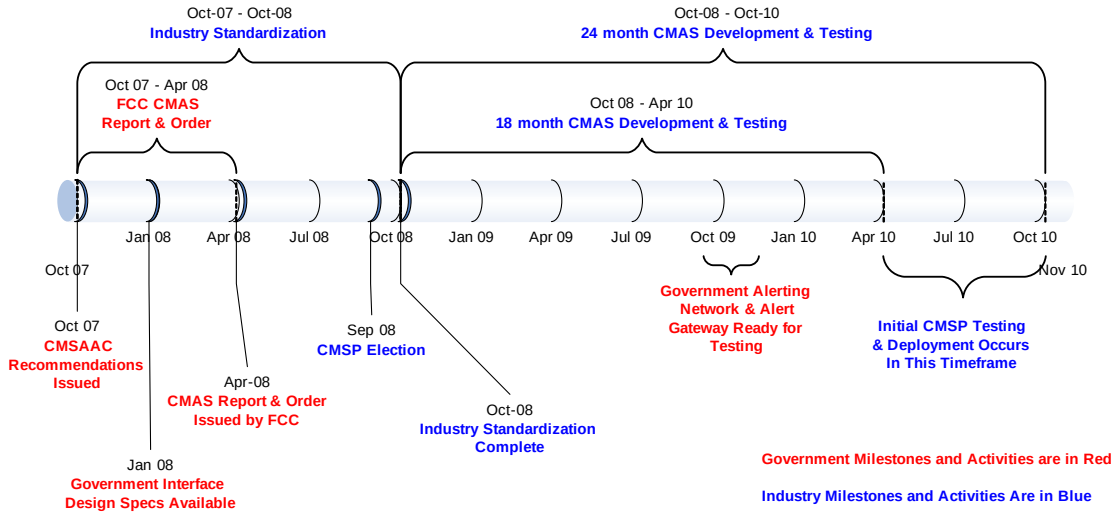

Figure 12-1 Potential Deployment Timeline

The above potential deployment timeline is based upon the assumptions that (1) the CMSAAC recommendations of PMG-035 are accepted without any major technical changes and (2) the government documentation and deliverables are available at the milestone dates indicated on the timeline. The industry will begin standardization efforts at the completion of the CMSAAC recommendations but any major technical changes to the CMSAAC recommendations will adversely affect the above potential deployment timeline.

There are factors outside of the CMSP's direct control that will influence the deployment and availability of CMA service. These factors include manufacturer development cycles for equipment in the CMSP infrastructure, manufacturer commitment to support the delivery technology of choice by the CMSP, and mobile device manufacturer development of the required CMAS functionality on the mobile devices. Typically, a CMSP will have equipment from multiple manufacturers deployed in the CMSP infrastructure. Multi-vendor environments require feature availability and deployment alignment, and require interoperability testing between the different manufacturers equipment. Also, if a CMSP chooses a particular technology to be used to transmit alerts (e.g., cell broadcast), if a vendor with which a CMSP has a relationship chooses not to develop the capability, then the CMSP may be forced into not electing to transmit alerts (at least not "in whole").

It is also assumed the requirements, development, and deployments of the Alert Gateway and Alert Aggregator align with the CMSP developments to allow for testing during the development process and prior to CMAS deployments.

12.3 Licensees and Permittees of Noncommercial Educations Broadcasting Stations or Public Television Stations

The WARN Act requires in section 602(c) that:

> Within 90 days after the date on which the Commission adopts relevant technical standards based on recommendations of the Commercial Mobile Service Alert Advisory Committee, established pursuant to section 603(a), the Commission shall complete a proceeding to require licensees and permittees of noncommercial educational broadcast stations or public broadcast stations (as those terms are defined in section 397(6) of the Communications Act of 1934 (47 U.S.C. 397(6))) to install necessary equipment and technologies on, or as part of, any broadcast television digital signal

> transmitter to enable the distribution of geographically targeted alerts by commercial mobile service providers that have elected to transmit emergency alerts under this section.

This Committee acknowledges the potential relevance of the rulemaking described in section 602(c) of the WARN Act to this Committee's recommendations. Accordingly, the Committee recommends that the equipment and technologies described in section 602(c) of the WARN Act be deployed promptly and in a manner consistent with the Committee's recommendations. The Committee further recommends that the national organization representing the licensees and permittees of non-commercial broadcast stations work with the FCC pursuant to Section 602(c) on the necessary equipment.