ATIS STANDARD

ATIS-0700035

ATIS Standard on -

Wireless Emergency Alert (WEA) 3.0 Service Description

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF NOR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to https://www.atis.org/policy/patent-assurances/ to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Published by

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

ATIS-0700035

ATIS Standard on

Wireless Emergency Alert (WEA) 3.0 Service Description

Alliance for Telecommunications Industry Solutions

Approved October 27, 2022

Abstract

This document provides a service description of the enhancements made to Wireless Emergency Alert (WEA) as identified in FCC Report and Order publications made in the September 2016, January 2017, and June 2021.

Foreword

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

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

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

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

M. Younge, WTSC Chair (T-Mobile USA)

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

T. Brooks, WTSC SN Chair (T-Mobile USA)

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

N. Rao, Technical Editor (Nokia)

The Systems & Networks (SN) subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

ATIS Standard on –

Wireless Emergency Alert (WEA) 3.0 Service Description

Preface

The authority-to-individual emergency alerting capability to mobile devices was originally called Commercial Mobile Alert System (CMAS) in the first three Reports and Orders from the FCC. Regulatory terminology was originally based upon the CMAS terminology and CMAS was operational in April 2012. However, in February 2013, the FCC renamed Commercial Mobile Alert System (CMAS) to Wireless Emergency Alerts (WEA) with associated updates to the appropriate sections of Part 11 of the 47 CFR. Subsequently, the FCC has issued additional enhancements and rules for this government-to-individual emergency alerting capability to mobile devices and these are identified as modifications to WEA.

Consequently, this specification may use both the term CMAS and the term WEA. These terms should be considered as equivalent terms with WEA being the preferred term.

With the September 2016 FCC Report and Order and Further Notice of Proposed Rulemaking [Ref 1], WEA was renamed in ATIS specifications to WEA 2.0, thereby renaming “legacy WEA” to WEA 1.0. With the January 2018 FCC Second Report and Order and Second Order on Reconsideration [Ref 2] the name WEA 3.0 was introduced. Consequently, the term WEA should be considered as equivalent with WEA 3.0 unless specifically mentioned otherwise.

1 Scope, Purpose, & Application

1.1 Scope

This document contains descriptions on how WEA operates. The requirements for WEA interfaces, network elements, and mobile devices are defined in other ATIS Standards, see Annex A.

1.2 Purpose

The purpose of this document is to provide a service description of WEA 3.0 based upon the WEA enhancements identified in the September 2016 FCC Report & Order on WEA Enhancements [Ref 1] and any other identified WEA enhancements. The information contained in this document will assist the reader on understanding the relationships between the various WEA standards (see Clauses A.3, A.4, and A.5 of Annex A).

1.3 Application

This Standard is applicable to Commercial Mobile Service Providers (CMSPs), the Federal government entity responsible for the administration of the Federal Alert Gateway, the CMSP infrastructure providers, the mobile device manufacturers, the non-commercial educational (NCE) and public broadcast television station licensees, and the Alert Originators.

2 References

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

[Ref 1] FCC 16-127, *Federal Communications Commission Report and Order and Further Notice of Proposed Rulemaking In the Matter of Wireless Emergency Alerts Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System*; September 29, 2016.[1]

[Ref 2] FCC 18-4, *Second Report and Order and Second Order on Reconsideration*; January 30, 2018[1]

[Ref 3] FCC 21-77, *Report and Order and Further Notice of Proposed Rulemaking In the Matter of Wireless Emergency Alerts Amendments of Part 11 of the Commission's Rules Regarding the Emergency Alert System;* June 17, 2021. [1]

[Ref 4] ATIS-0700036, *Wireless Emergency Alert (WEA) 3.0 Mobile Device Behavior (MDB) Specification*.[2]

[Ref 5] ATIS-0700041, *Wireless Emergency Alerts (WEA) 3.0: Device-Based Geo-Fencing.*[2]

NOTE: The complete set of WEA 3.0 specifications are contained in Annex A.

3 Definitions, Acronyms, & Abbreviations

3.1 Definitions

Alert Area: The area that the Alert Originator identifies for alert dissemination. This may be defined by geocode only, or by geocode and one or more geometric shapes (polygon(s) and/or circle(s)).

Enhanced Wireless Emergency Alert (eWEA): A continued provision of effective WEA Alert Messages while leveraging advancements in technology to improve WEA's capabilities as defined in the September 29, 2016 FCC Report and Order on WEA Enhancements, FCC 16-127 [Ref 1].

NOTE: The Enhanced Wireless Emergency Alert (eWEA) is referred to as WEA 2.0 in this standard.

Warning Area Coordinates: The coordinates defining the polygon(s) and/or circle(s) that specify the alert's geographic boundary(ies), as provided by the alert originator.

3.2 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
ATIS	Alliance for Telecommunications Industry Solutions
DBGF	Device-Based Geo-Fencing
MDB	Mobile Device Behavior
CFR	Code of Federal Regulations
CMAC	Commercial Mobile Alert C-Interface
CMAS	Commercial Mobile Alert System
CMSP	Commercial Mobile Service Provider
eWEA	Enhanced Wireless Emergency Alert
FCC	Federal Communications Commission
FNPRM	Further Notice of Proposed Rulemaking
ID	Identity
NCE	Non-Commercial Educational

[1] This document is available from the Federal Communications Commission. < http://www.fcc.gov/ >

[2] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS). < http://www.atis.org >

PSA	Public Service Announcements
PWS	Public Warning System
R&O	Report & Order
US	United States
WARN	Warning, Alert, & Response Network
WEA	Wireless Emergency Alert

4 Definition of WEA Enhancements

In the September 2016 FCC Report & Order on WEA enhancements, FCC 16-127 [Ref 1], the FCC defined regulatory changes for WEA enhancements. Some of these WEA enhancements are new regulatory requirements and some are modifications to existing WEA regulations. A summary of the WEA regulations before the September 2016 Report & Order [Ref 1] is provided in Annex B.

The January 2018 FCC Second Report and Order and Second Order on Reconsideration, FCC 18-4 [Ref 2] is the basis for the WEA 3.0 specifications.

The June 2021 FCC Report and Order and Further Notice of Proposed Rulemaking, FCC 21-77 [Ref 3], re-designates WEA Presidential Alerts to include alerts from both the President and from the FEMA Administrator, and renames the Presidential Alert to National Alert.

4.1 FCC Report & Order Mandated WEA Enhancements

The following table provides a summary of the WEA enhancements from the September 2016 FCC Report & Order, FCC 16-127 [Ref 1]. For the full text of the WEA enhancements, refer to discussion paragraphs in the FCC Report & Order FCC 16-127 [Ref 1] and the 47 CFR sections as specified in *Appendix A Final Rules* of the FCC Report & Order FCC 16-127 [Ref 1].

Table 4-1: Summary of FCC Report & Order 16-127 Mandated WEA Enhancements

WEA Enhancement	Enhancement Definition	Reference to FCC R&O FCC 16-127 [Ref 1]
Increasing Maximum WEA Character Length	Increase alert text to a maximum of 360 characters of alphanumeric on 4G, 5G and future networks. Continue to allow the delivery of 90-character messages on 2G & 3G networks. Participating CMS Provider must support transmission of an Alert Message that contains a maximum of 90 characters of alphanumeric text on (and only on) those network elements that are incapable of supporting a 360-character Alert Message.	R&O Section III.A.1 47 CFR § 10.430 amended

WEA Enhancement	Enhancement Definition	Reference to FCC R&O FCC 16-127 [Ref 1]
Classifying Public Safety Messages	Public Safety Message is defined as "an essential public safety advisory that prescribes one or more actions likely to save lives and/or safeguard property". Public Safety Messages will only be eligible for issuance in connection with an Imminent Threat Alert, an AMBER Alert, or a Presidential Alert. NOTE: Public Safety Messages are **not** eligible for issuance in connection with State/Local WEA Testing. Participating CMS Providers shall provide for their subscribers to receive Public Safety Messages by default, and may provide their subscribers with the option to opt out of receiving Public Safety Messages if they decide that they no longer wish to receive them. Does **not** require Participating CMS Providers to associate a unique attention signal or vibration cadence with Public Safety Messages.	R&O Section III.A.2 47 CFR § 10.280(a) amended 47 CFR § 10.400(d) amended 47 CFR § 10.410 amended
Supporting Embedded References and Multimedia	Removes restriction on embedded references as specified in the FCC First Report & Order, FCC 08-099. Participating CMS Providers must support the transmission of embedded URLs and phone numbers in WEA Alert Messages.	R&O Section III.A.3 47 CFR § 10.440 removed 47 CFR § 10.441 added
Spanish-language Alerting	Section 10.500(e) from the First R&O requires mobile devices to be able to extract Alert Message content in the subscriber's preferred language. Participating CMS Providers are required to transmit WEA Alert Messages that are issued in the Spanish language or that contain Spanish-language characters.	R&O Section III.A.4 47 CFR § 10.480 added

WEA Enhancement	Enhancement Definition	Reference to FCC R&O FCC 16-127 [Ref 1]
Alert Logging	The CMS provider gateway must perform the following functions: (1) **Logging Requirements.** Log the CMAC (Commercial Mobile Alert C-Interface) attributes of all Alert Messages received at the CMS Provider Alert Gateway, including time stamps that verify when the message is received, and when it is retransmitted or rejected by the Participating CMS Provider Alert Gateway. If an Alert Message is rejected, a Participating CMS Provider is required to log the specific error code generated by the rejection. (2) **Maintenance of Logs.** Participating CMS Providers are required to maintain a log of all active and cancelled Alert Messages for at least 12 months after receipt of such alert or cancellation. (3) **Availability of Logs.** Participating CMS Providers are required to make their alert logs available to the Commission and FEMA upon request. Participating CMS Providers are also required to make alert logs available to emergency management agencies that offer confidentiality protection at least equal to that provided by the federal Freedom of Information Act (FOIA) upon request, but only insofar as those logs pertain to Alert Messages initiated by that emergency management agency. Does **not** require Participating CMS Providers to take a uniform approach to alert logging today, only that they log the relevant information, maintain that information and make it available to appropriate parties. Does **not** require Participating CMS Providers support an automated transmission of alert log data to emergency managers' alert origination software.	R&O Section III.B.1 47 CFR § 10.320(g) added
WEA Geo-targeting	Participating CMS Provider must transmit any Alert Message that is specified by a geocode, circle, or polygon to an area that best approximates the specified geocode, circle, or polygon. If, however, the Participating CMS Provider cannot broadcast the Alert Message to an area that best approximates the specified geocode, circle, or polygon, a Participating CMS Provider may transmit an Alert Message to an area not larger than the propagation area of a single transmission site. Upon request from an emergency management agency, a Participating CMS Provider will disclose information regarding their capabilities for geo-targeting Alert Messages. This is out of scope of the ATIS standards.	R&O Section III.B.2 47 CFR § 10.450 amended

WEA Enhancement	Enhancement Definition	Reference to FCC R&O FCC 16-127 [Ref 1]
WEA Presentation	Mobile devices must present an Alert Message as soon as they receive it, but mobile device may **not** enable an Alert Message to preempt an active voice or data session. WEA-capable mobile devices engaged in active voice or data sessions on 2G & 3G networks may not be able to receive available Alert Messages until the active voice or data session concludes. If a mobile device receives a WEA Alert Message during an active voice or data session, the user may be given the option to control how the Alert Message is presented on the mobile device with respect to the use of the common vibration cadence and audio attention signal.	R&O Section III.B.3 47 CFR § 10.510 amended
State/Local WEA Testing	A Participating CMS Provider must support State/Local WEA Tests. (1) A Participating CMS Provider's Gateway shall support the ability to receive a State/Local WEA Test message. (2) A Participating CMS Provider shall immediately transmit a State/Local WEA Test to the geographic area specified by the alert originator. (3) A Participating CMS Provider may forego a State/Local WEA Test if the State/Local WEA Test is pre-empted by actual alert traffic or if an unforeseen condition in the CMS Provider infrastructure precludes distribution of the State/Local WEA Test. If a Participating CMS Provider Gateway forgoes a State/Local WEA Test, it shall send a response code to the Federal Alert Gateway indicating the reason. (4) Participating CMS Providers shall provide their subscribers with the option to opt in to receive State/Local WEA Tests. A CMS Provider may not forego or delay delivery of a State/Local WEA Test message except when the test is preempted by actual Alert message traffic, or if an unforeseen condition in the Participating CMS Provider infrastructure precludes distribution of the State/Local WEA Test. Consumers will not receive State/Local WEA Tests by default. The default configuration on mobile devices for State/Local WEA test is opt-out. The consumer must opt in to receive the State/Local WEA tests. State/Local WEA Tests are required to include conspicuous language sufficient to make clear to the public that the message is, in fact, only a test. This is a requirement for the Alert Originators and not a requirement for the CMSPs. Therefore, this is out of scope for the ATIS standards.	R&O Section III.C.1 47 CFR § 10.350(c) added
C interface Backup Testing	Not applicable to ATIS standards.	R&O Section III.C.2 47 CFR § 10.350(b) amended

WEA Enhancement	Enhancement Definition	Reference to FCC R&O FCC 16-127 [Ref 1]
WEA PSAs	Not applicable to ATIS standards.	R&O Section III.C.3 47 CFR § 10.520(d) amended

The following table provides a summary of the WEA enhancements from the January 2018 FCC Second Report and Order and Second Order on Reconsideration, FCC 18-4 [Ref 2]. For the full description of the WEA enhancements, refer to discussion paragraphs in the FCC Second Report and Order and Second Order on Reconsideration, FCC 18-4 [Ref 2], and the 47 CFR sections as specified in *Appendix A Final Rules* of the FCC Report & Order FCC 18-4 [Ref 2].

Table 4-2: Summary of FCC Report & Order Mandated 18-4 WEA Enhancements

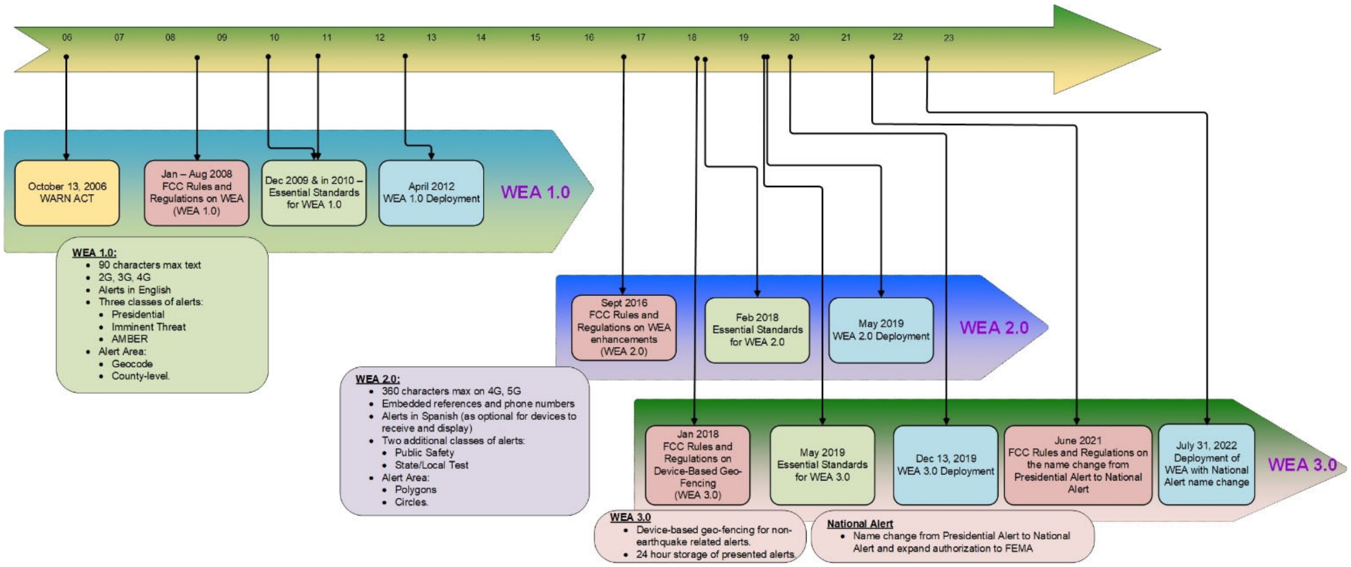
WEA Enhancement	Enhancement Definition	Reference to FCC R&O FCC 18-4 [Ref 2]
Narrowing Geo-Targeting Requirements	CMSPs are required to deliver Alert Messages to an area that matches the target area specified by alert originators to 100 percent of the target area with no more than 0.1 of a mile overshoot.	R&O Section III.A.2
Alert Message Preservation	WEA-capable mobile devices must preserve Alert Messages in a consumer-accessible format and location for at least 24 hours after the Alert Message is received on the subscriber's mobile device, or until deleted by the subscriber.	R&O Section III.A.3 47 CFR § 10.500 amended

The following table provides a summary of the WEA enhancements from the June 2021 FCC Second Report and Order and Further Notice of Proposed Rulemaking, FCC 21-77 [Ref 3]. For the full description of the WEA enhancements, refer to discussion paragraphs in the FCC Second Report and Order and Further Notice of Proposed Rulemaking, FCC 21-77 [Ref 3].

Table 4-3: Summary of FCC Report & Order Mandated 21-77 WEA Enhancements

WEA Enhancement	Enhancement Definition	Reference to FCC R&O FCC 21-77 [Ref 3]
National Alert	Introduced a new class of WEA National Alert that replaces the Presidential Alert and now includes the alerts generated by FEMA administrators.	R&O Section III.A

4.2 Chronological View of WEA progress


06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21
22
23
October 13, 2006 WARN ACT
Jan – Aug 2008 FCC Rules and Regulations on WEA (WEA 1.0)
Dec 2009 & in 2010 – Essential Standards for WEA 1.0
April 2012 WEA 1.0 Deployment
WEA 1.0
Sept 2016 FCC Rules and Regulations on WEA enhancements (WEA 2.0)
Feb 2018 Essential Standards for WEA 2.0
May 2019 WEA 2.0 Deployment
WEA 2.0
Jan 2018 FCC Rules and Regulations on Device-Based Geo-Fencing (WEA 3.0)
May 2019 Essential Standards for WEA 3.0
Dec 13, 2019 WEA 3.0 Deployment
June 2021 FCC Rules and Regulations on the name change from Presidential Alert to National Alert
July 31, 2022 Deployment of WEA with National Alert name change
WEA 3.0

WEA 1.0:

- 90 characters max text
- 2G, 3G, 4G
- Alerts in English
- Three classes of alerts:
  - Presidential
  - Imminent Threat
  - AMBER
- Alert Area:
  - Geocode
  - County-level.

WEA 2.0:

- 360 characters max on 4G, 5G
- Embedded references and phone numbers
- Alerts in Spanish (as optional for devices to receive and display)
- Two additional classes of alerts:
  - Public Safety
  - State/Local Test
- Alert Area:
  - Polygons
  - Circles.

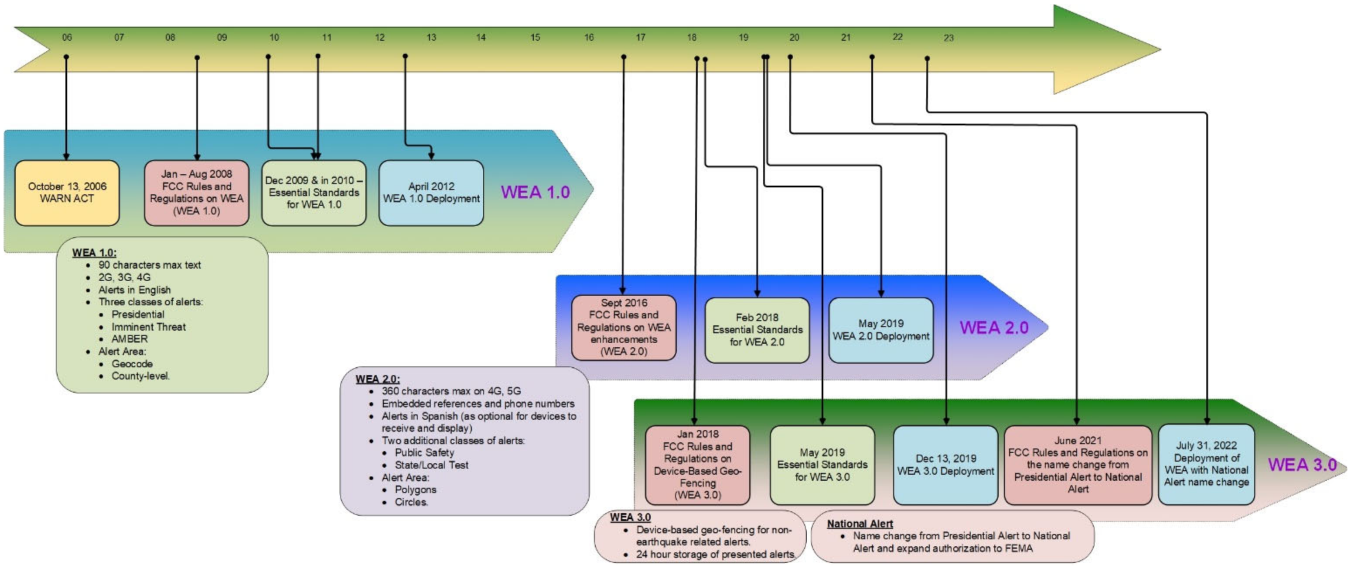
WEA 3.0

- Device-based geo-fencing for non-earthquake related alerts.
- 24 hour storage of presented alerts.

National Alert

- Name change from Presidential Alert to National Alert and expand authorization to FEMA

Figure 4-1 shown below shows the progress of WEA in the industry from the FCC regulations to standardization to deployment stages.



06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21
22
23
October 13, 2006 WARN ACT
Jan – Aug 2008 FCC Rules and Regulations on WEA (WEA 1.0)
Dec 2009 & in 2010 – Essential Standards for WEA 1.0
April 2012 WEA 1.0 Deployment
WEA 1.0
Sept 2016 FCC Rules and Regulations on WEA enhancements (WEA 2.0)
Feb 2018 Essential Standards for WEA 2.0
May 2019 WEA 2.0 Deployment
WEA 2.0
Jan 2018 FCC Rules and Regulations on Device-Based Geo-Fencing (WEA 3.0)
May 2019 Essential Standards for WEA 3.0
Dec 13, 2019 WEA 3.0 Deployment
June 2021 FCC Rules and Regulations on the name change from Presidential Alert to National Alert
July 31, 2022 Deployment of WEA with National Alert name change
WEA 3.0
WEA 1.0: 90 characters max text; 2G, 3G, 4G; Alerts in English; Three classes of alerts: Presidential, Imminent Threat, AMBER; Alert Area: Geocode, County-level.
WEA 2.0: 360 characters max on 4G, 5G; Embedded references and phone numbers; Alerts in Spanish (as optional for devices to receive and display); Two additional classes of alerts: Public Safety, State/Local Test; Alert Area: Polygons, Circles.
WEA 3.0: Device-based geo-fencing for non-earthquake related alerts. 24 hour storage of presented alerts.
National Alert: Name change from Presidential Alert to National Alert and expand authorization to FEMA

Figure 4-1: Chronological view of WEA progress

As shown in

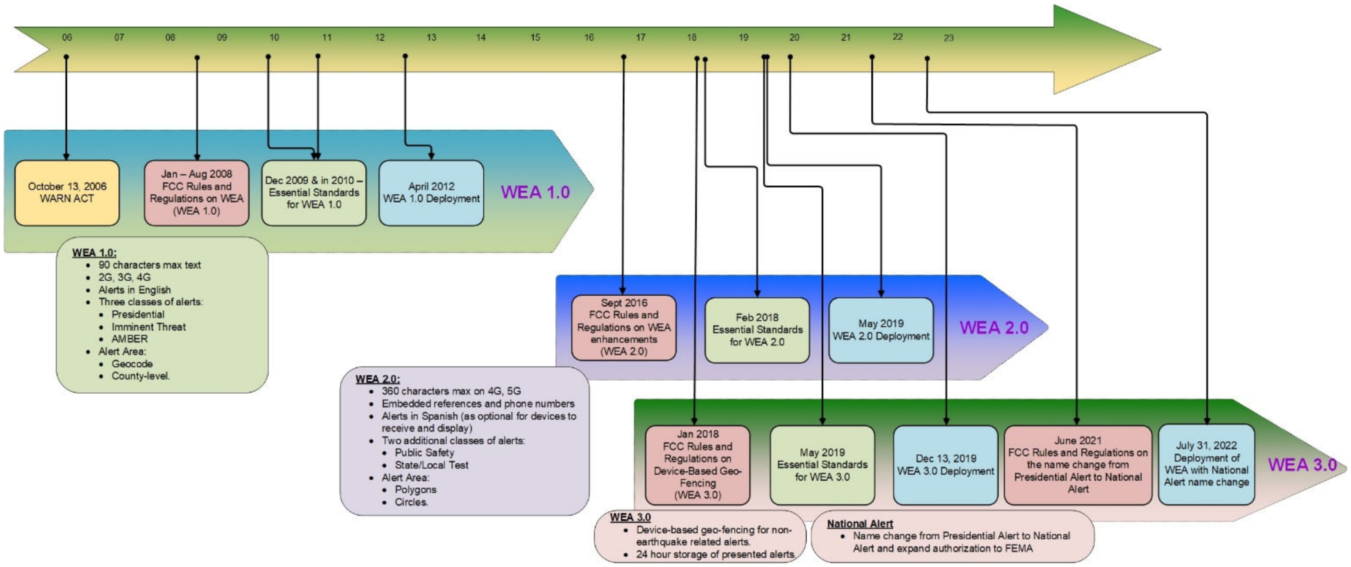

06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21
22
23
October 13, 2006 WARN ACT
Jan – Aug 2008 FCC Rules and Regulations on WEA (WEA 1.0)
Dec 2009 & in 2010 – Essential Standards for WEA 1.0
April 2012 WEA 1.0 Deployment
WEA 1.0
WEA 1.0:
90 characters max text
2G, 3G, 4G
Alerts in English
Three classes of alerts:
Presidential
Imminent Threat
AMBER
Alert Area:
Geocode
County-level.
Sept 2016 FCC Rules and Regulations on WEA enhancements (WEA 2.0)
Feb 2018 Essential Standards for WEA 2.0
May 2019 WEA 2.0 Deployment
WEA 2.0
WEA 2.0:
360 characters max on 4G, 5G
Embedded references and phone numbers
Alerts in Spanish (as optional for devices to receive and display)
Two additional classes of alerts:
Public Safety
State/Local Test
Alert Area:
Polygons
Circles.
Jan 2018 FCC Rules and Regulations on Device-Based Geo-Fencing (WEA 3.0)
May 2019 Essential Standards for WEA 3.0
Dec 13, 2019 WEA 3.0 Deployment
June 2021 FCC Rules and Regulations on the name change from Presidential Alert to National Alert
July 31, 2022 Deployment of WEA with National Alert name change
WEA 3.0
WEA 3.0
Device-based geo-fencing for non-earthquake related alerts.
24 hour storage of presented alerts.
National Alert
Name change from Presidential Alert to National Alert and expand authorization to FEMA

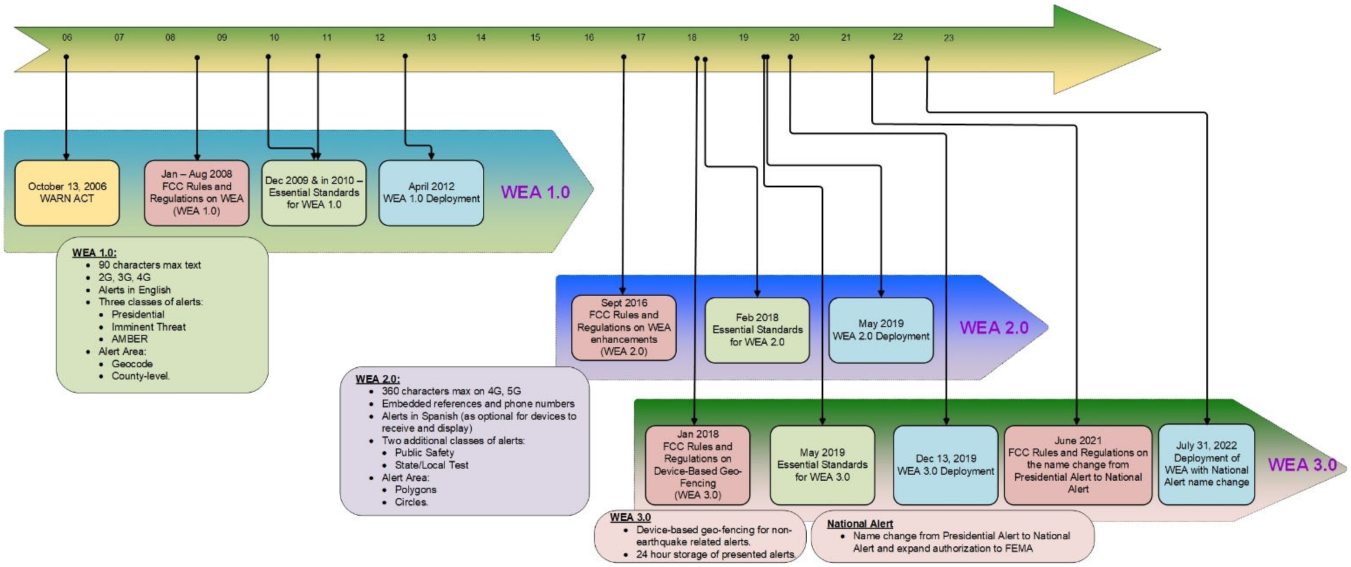
Figure 4-1, the WEA deployment has happened within the industry in three phases: WEA 1.0, WEA 2.0, and WEA 3.0.

WEA 1.0 is based on the FCC regulations that were published in several phases between January and August of 2008 and is being deployed within the CMSP networks since April of 2012.

WEA 2.0 is based on the FCC regulations that were published in September of 2016 and is being deployed since May of 2019.

WEA 3.0 is based on the FCC regulations that were published in January of 2018 and is deployed since December 2019.

The FCC published a new regulation in June of 2021 [Ref 3] to rename the Presidential Alert to National Alert and to re-designate it to include alerts from both the President and the FEMA Administrator, to be deployed by July of 2022. Even though shown under the WEA 3.0 path in



06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21
22
23
October 13, 2006 WARN ACT
Jan – Aug 2008 FCC Rules and Regulations on WEA (WEA 1.0)
Dec 2009 & in 2010 – Essential Standards for WEA 1.0
April 2012 WEA 1.0 Deployment
WEA 1.0
WEA 1.0:
90 characters max text
2G, 3G, 4G
Alerts in English
Three classes of alerts:
Presidential
Imminent Threat
AMBER
Alert Area:
Geocode
County-level.
Sept 2016 FCC Rules and Regulations on WEA enhancements (WEA 2.0)
Feb 2018 Essential Standards for WEA 2.0
May 2019 WEA 2.0 Deployment
WEA 2.0
WEA 2.0:
360 characters max on 4G, 5G
Embedded references and phone numbers
Alerts in Spanish (as optional for devices to receive and display)
Two additional classes of alerts:
Public Safety
State/Local Test
Alert Area:
Polygons
Circles.
Jan 2018 FCC Rules and Regulations on Device-Based Geo-Fencing (WEA 3.0)
May 2019 Essential Standards for WEA 3.0
Dec 13, 2019 WEA 3.0 Deployment
June 2021 FCC Rules and Regulations on the name change from Presidential Alert to National Alert
July 31, 2022 Deployment of WEA with National Alert name change
WEA 3.0
WEA 3.0
Device-based geo-fencing for non-earthquake related alerts.
24 hour storage of presented alerts.
National Alert
Name change from Presidential Alert to National Alert and expand authorization to FEMA

Figure 4-1, the name change is independent of the three WEA phases.

4.3 *Applicability of WEA Enhancements to LTE and 5G Networks*

The following table identifies the WEA enhancements that are limited to the LTE and 5G networks per the FCC Report & Order on WEA enhancements, FCC 16-127 [Ref 1] and the FCC Second Report and Order and Second Order on Reconsideration, FCC 18-4 [Ref 2]:

Table 4-4: WEA Enhancements Limited to LTE and 5G by FCC R&O 16-127 [Ref 1], 18-4 [Ref 2], 21-77 [Ref 3]

WEA Enhancement as Quoted in FCC 16-127 [Ref 1], FCC 18-4 [Ref 2] and FCC 21-77 [Ref 3]	Limited to LTE and 5G by R&O
Increasing Maximum WEA Character Length	Yes
Classifying Public Safety Messages	No
Supporting Embedded References and Multimedia	No
Spanish-language Alerting	No
Alert Logging	No
WEA Geo-targeting (FCC 16-127 [Ref 1])	No
WEA Presentation	Yes
State/Local WEA Testing	No
Narrowing Geo-targeting (FCC 18-4 [Ref 2])	Yes
Message Preservation	No
National Alert	No

5 WEA Service Description Architecture

Figure 5-1 below provides a high-level WEA architecture diagram. An Alerting Authority, also known as an Alert Originator, determines that a WEA needs to be sent to the public in a particular alerting area. The alert information is sent across the A interface to the FEMA-administered Integrated Public Alert and Warning System (IPAWS) Open Platform for Emergency Networks (OPEN) which provides alert aggregation and alert dissemination functions. The IPAWS OPEN system provides a C interface formatted alert to the Commercial Mobile Service Provider (CMSP) Gateway as well as to the Public Broadcasting Service (PBS) Warning Alert Response Network (WARN) system. The PBS WARN system provides a broadcast alert over the C1 interface as a backup transmission method that may be used by the CMSP Gateway in the event that the C interface link between IPAWS OPEN and the CMSP Gateway is compromised. The CMSP infrastructure provides for geotargeting of the alert and broadcasts the alert in the best approximation of the relevant alert area over the E (cellular radio) interface. Mobile devices in the broadcast area may perform Device-Based Geo-Fencing (DBGF) to further assist with accurate geotargeting of the alert.

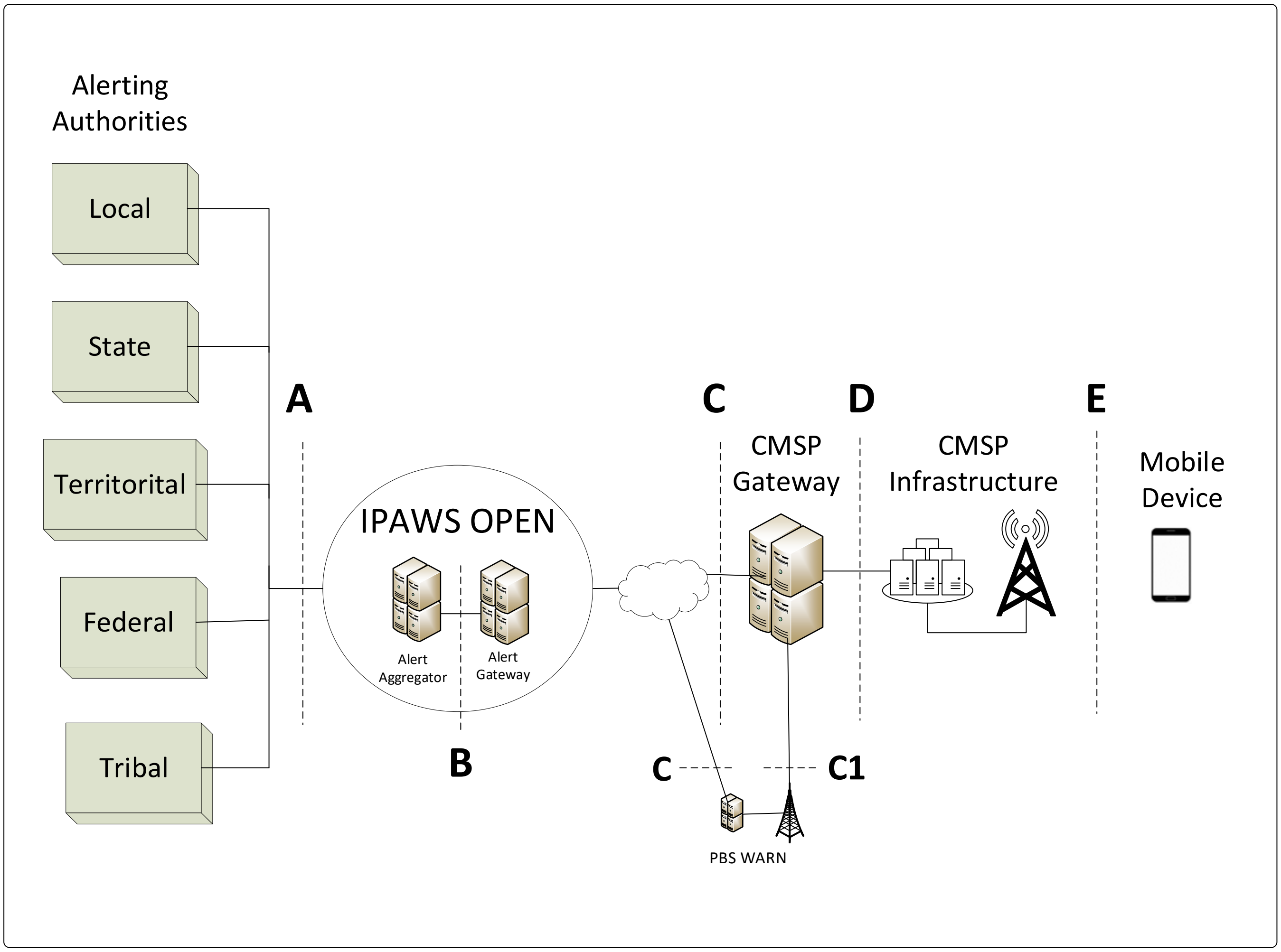


Figure 5-1: High-Level WEA Architecture

The B interface shown in Figure 5-1 is an internal interface within IPAWS OPEN between the Alert Aggregator and the Alert Gateway. The details of A and B interfaces are outside the scope of ATIS standards.

6 General WEA Principles

6.1 Alert Classes & Associated Opt-In/Opt-Out Capabilities

Prior to the September 2016 FCC WEA Enhancements Report & Order FCC 16-127 [Ref 1], alerts were divided into the following three WEA alert classes with the associated presentation and subscriber opt-in / opt-out characteristics:

- **National Alert**
  - Always presented when received.
  - Subscriber's mobile device has no options to opt-in / opt-out of National alerts.

- **Imminent Threat Alert**
  - Presented based upon subscriber's opt-in / opt-out selections.

  - Default mobile device configuration is opt-in.
  - Subscriber’s mobile device has configuration options to opt-in / opt-out of all or potentially some types of Imminent Threats.

- **AMBER Alert**
  - Presented based upon subscriber’s opt-in / opt-out selection.
  - Default mobile device configuration is opt-in.
  - Subscriber’s mobile device has a configuration option to opt-in / opt-out of AMBER alerts.

The WEA enhancements of FCC Report & Order FCC 16-127 [Ref 1] include two new WEA alert classes for State/Local WEA Testing and for Public Safety messages. The presentation and opt-in/opt-out characteristics of the above three WEA alert classes remain unchanged. The two new WEA alert classes have the following presentation and opt-in / opt-out characteristics:

- **State/Local WEA Test**
  - Presented based upon subscriber’s opt-in / opt-out selection.
  - Default mobile device configuration is opt-out.
  - Subscriber’s mobile device has a configuration option to opt-in / opt-out of State/Local WEA Test alerts.

- **Public Safety Alert**
  - Presented based upon subscriber’s opt-in / opt-out selection.
  - Default mobile device configuration is opt-in.
  - Subscriber’s mobile device has a configuration option to opt-in / opt-out of Public Safety alerts.

In the following sections which describe various scenarios that lead to presentation of alerts on the mobile device, it is assumed that the user has opted in for the class of alert being received.

6.2 WEA Alerts with Multiple Lengths & Multiple Languages

6.2.1 General Principles for Multiple Lengths

With WEA messages in multiple lengths, the Alert Originator is expected to construct the short text (90-characters maximum) text and long text (360-characters maximum).

An end-to-end view of WEA message flow with short text and long text in English is illustrated in Figure 6-1 below.

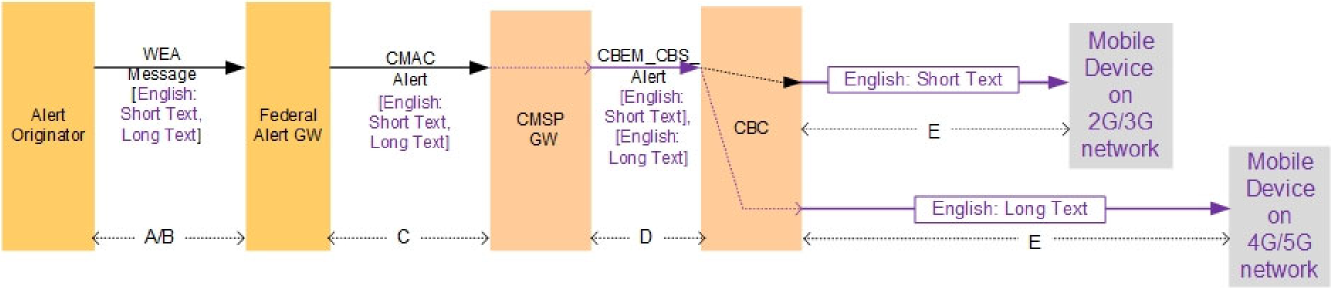

Alert Originator
WEA Message [English: Short Text, Long Text]
Federal Alert GW
CMAC Alert [English: Short Text, Long Text]
CMSP GW
CBEM_CBS Alert [English: Short Text], [English: Long Text]
CBC
English: Short Text
Mobile Device on 2G/3G network
E
English: Long Text
Mobile Device on 4G/5G network
A/B
C
D
E

Figure 6-1: Short and Long Message Flow

The Alert Originator sends the WEA message that contains the short text and long text to the Federal Alert Gateway.

The Federal Alert Gateway forwards the WEA message that carries the short text and long text to the CMSP Gateway.

The CMSP Gateway forwards the WEA message to the CBC over the D interface.

The CBC splits and sends the WEA with short text toward mobile devices that receive messages over 2G/3G radio network and WEA with long text toward mobile devices that receive the WEA over 4G/5G radio network.

When a mobile device receives a repetition of a message with a particular combination of Message Identifier and Serial Number that it has already presented, it will not present the message again.

See flow in Figure 6-4 and

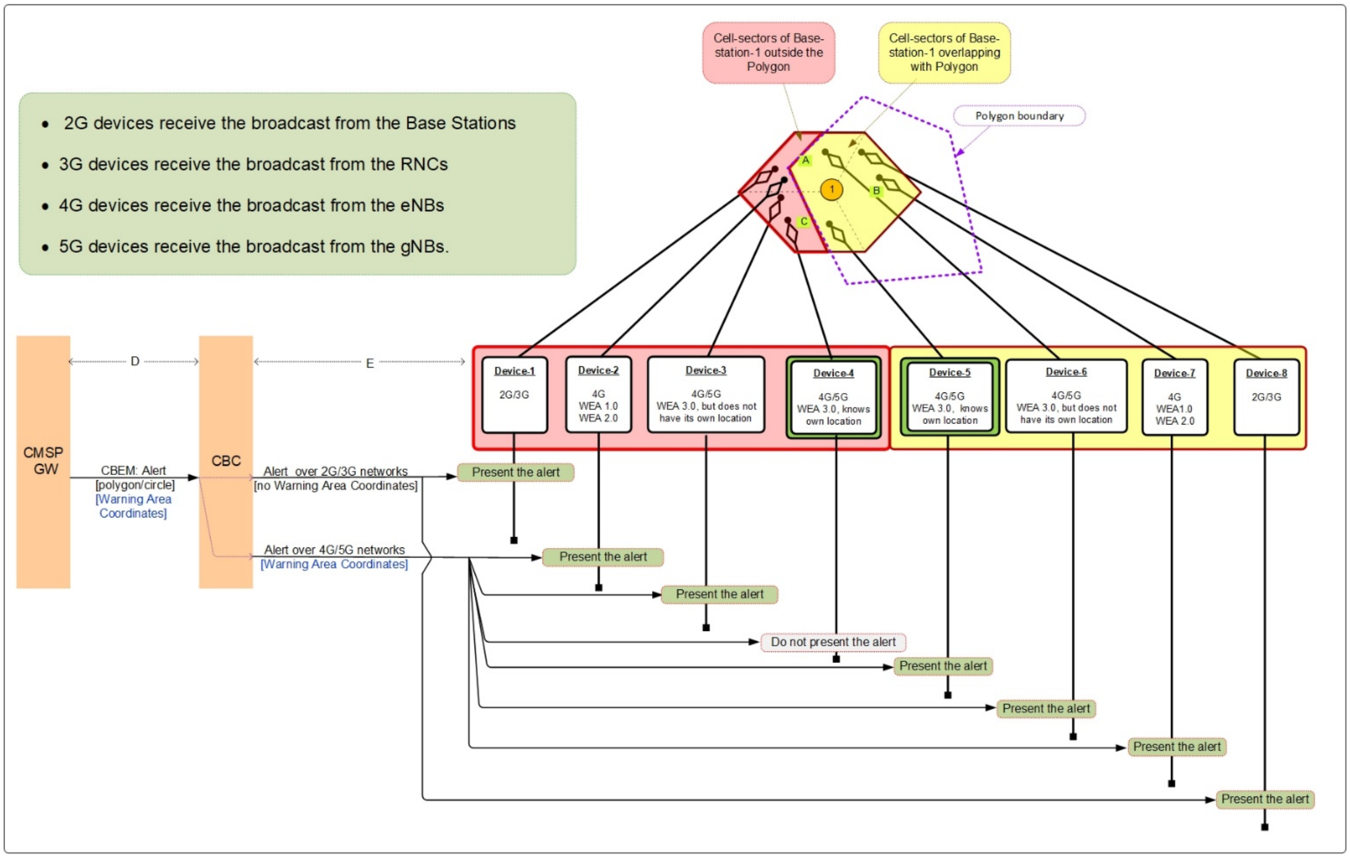

Cell-sectors of Base-station-1 outside the Polygon
Cell-sectors of Base-station-1 overlapping with Polygon
Polygon boundary
• 2G devices receive the broadcast from the Base Stations
• 3G devices receive the broadcast from the RNCs
• 4G devices receive the broadcast from the eNBs
• 5G devices receive the broadcast from the gNBs.
A
B
C
1
CMSP GW
D
CBC
E
CBEM: Alert [polygon/circle] [Warning Area Coordinates]
Alert over 2G/3G networks [no Warning Area Coordinates]
Alert over 4G/5G networks [Warning Area Coordinates]
Device-1 2G/3G
Device-2 4G WEA 1.0 WEA 2.0
Device-3 4G/5G WEA 3.0, but does not have its own location
Device-4 4G/5G WEA 3.0, knows own location
Device-5 4G/5G WEA 3.0, knows own location
Device-6 4G/5G WEA 3.0, but does not have its own location
Device-7 4G WEA1.0 WEA 2.0
Device-8 2G/3G
Present the alert
Present the alert
Present the alert
Do not present the alert
Present the alert
Present the alert
Present the alert
Present the alert

Figure 6-5 for the Device-Based Geo-Fencing (DBGF) aspects of WEA.

6.2.2 General Principles for Multiple Languages

Federal Alert Gateway will include English 90-character and 360-character, and may include Spanish 90-character and 360-character.

An end-to-end view of WEA message flow in English and Spanish is illustrated in Figure 6-2 below.

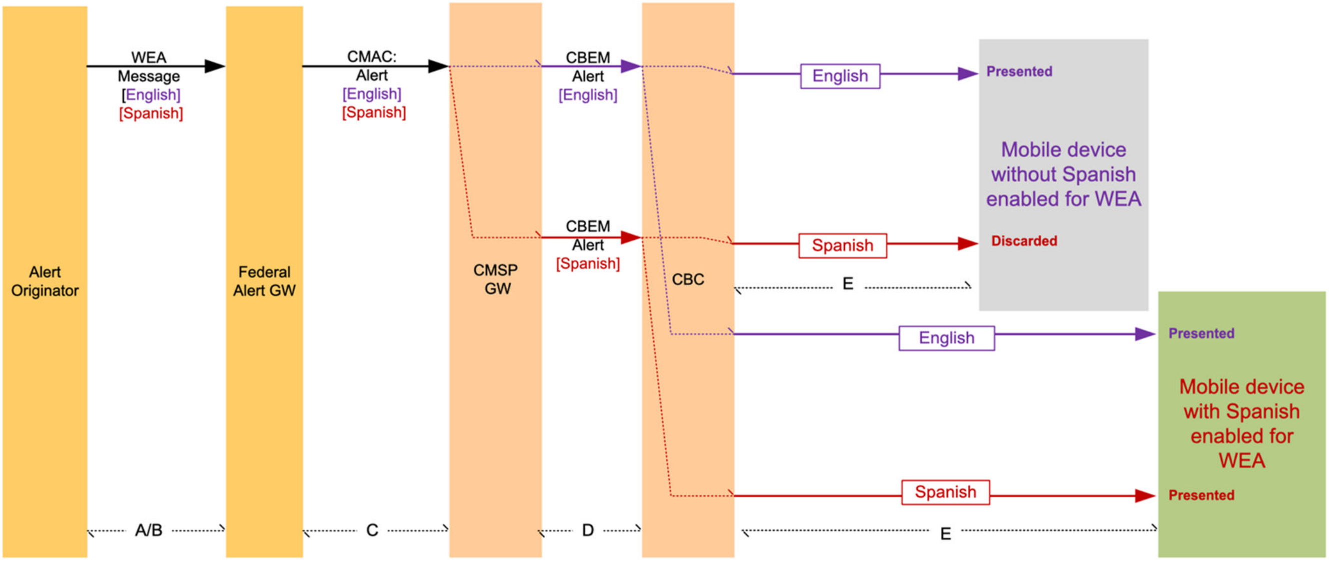


Figure 6-2: English and Spanish Message Flow

The Alert Originator sends the WEA message that carries alert text in English and the alert text in Spanish to the Federal Alert Gateway over the A/B interface.

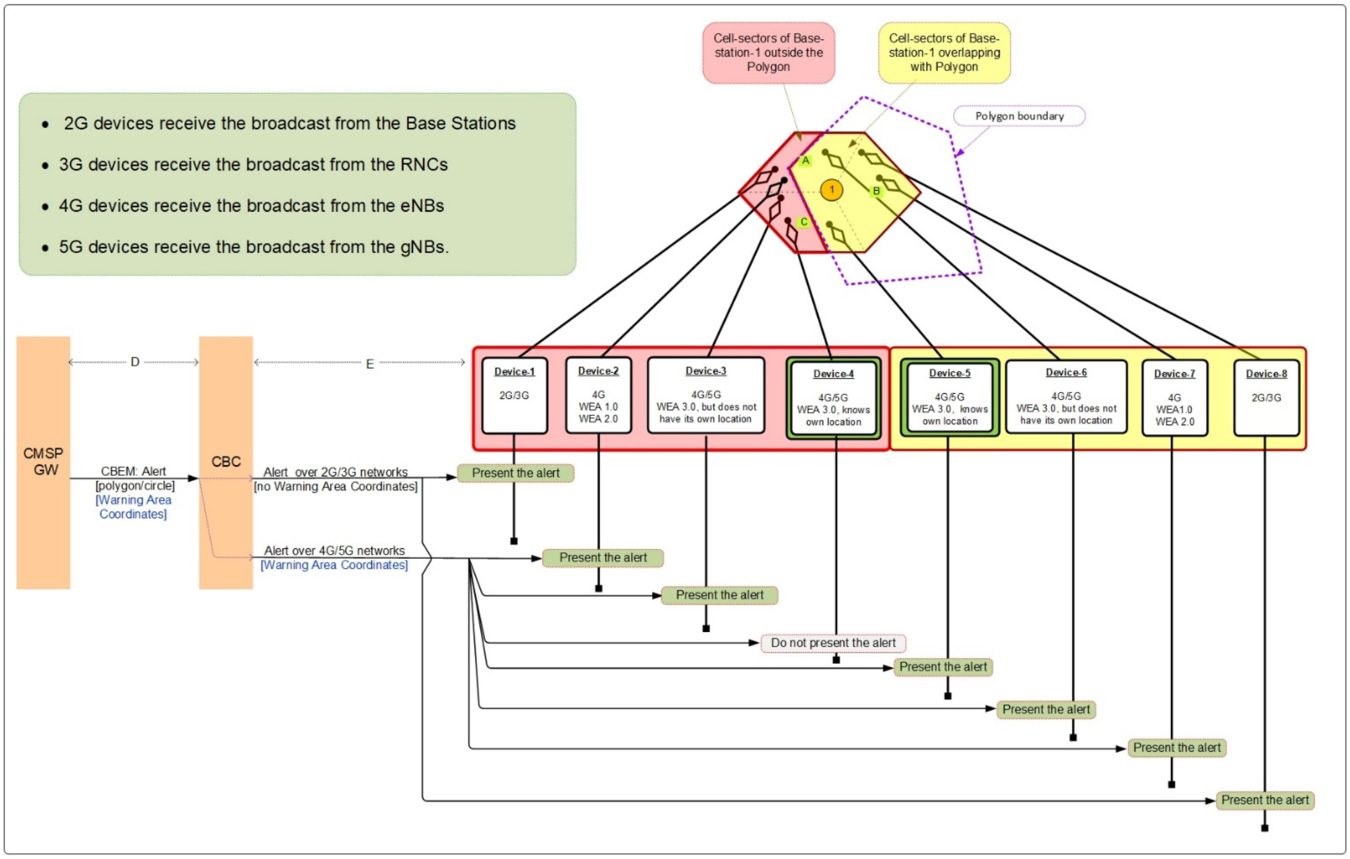
The Federal Alert Gateway forwards the WEA message that contains the alert text in English and the alert text in Spanish to the CMSP Gateway.

The CMSP Gateway splits the WEA message that contains the alert text in English and the alert text in Spanish into two independent alerts (as in Clause 6.2.3) one carrying the alert text in English and one carrying the alert text in Spanish and then sends each of them to the CBC over the D-interface.

The CBC sends each WEA, as received, toward the mobile devices.

The English alert text will always be presented by the device. If the mobile device user has Spanish enabled for WEA, the mobile device will also present the Spanish alert text.

> NOTE 1: A WEA Update message is handled by first cancelling the referenced English and Spanish WEAs messages and then transmitting the WEA with the updated English and Spanish text as new WEAs.
>
> NOTE 2: A WEA Update can be different from the initial WEA. For example, a WEA may have text in English and Spanish, whereas an WEA Update may have alert text only in English. In the same way, a WEA may have text in only English and the WEA Update may have text in English and Spanish.


Cell-sectors of Base-station-1 outside the Polygon
Cell-sectors of Base-station-1 overlapping with Polygon
Polygon boundary
2G devices receive the broadcast from the Base Stations
3G devices receive the broadcast from the RNCs
4G devices receive the broadcast from the eNBs
5G devices receive the broadcast from the gNBs.
A
1
B
C
D
E
CMSP GW
CBC
CBEM: Alert [polygon/circle] [Warning Area Coordinates]
Alert over 2G/3G networks [no Warning Area Coordinates]
Alert over 4G/5G networks [Warning Area Coordinates]
Device-1 2G/3G
Device-2 4G WEA 1.0 WEA 2.0
Device-3 4G/5G WEA 3.0, but does not have its own location
Device-4 4G/5G WEA 3.0, knows own location
Device-5 4G/5G WEA 3.0, knows own location
Device-6 4G/5G WEA 3.0, but does not have its own location
Device-7 4G WEA1.0 WEA 2.0
Device-8 2G/3G
Present the alert
Present the alert
Present the alert
Do not present the alert
Present the alert
Present the alert
Present the alert
Present the alert

See flow in Figure 6-4 and Figure 6-5 for the DBGF aspects of WEA.

6.2.3 Combined View of Multiple Lengths with Languages

This clause presents a combined view of WEA message broadcast showing short text and long text in English and Spanish.

An end-to-end view of WEA message flow with short text and long text in English and Spanish is illustrated in Figure 6-3 below.

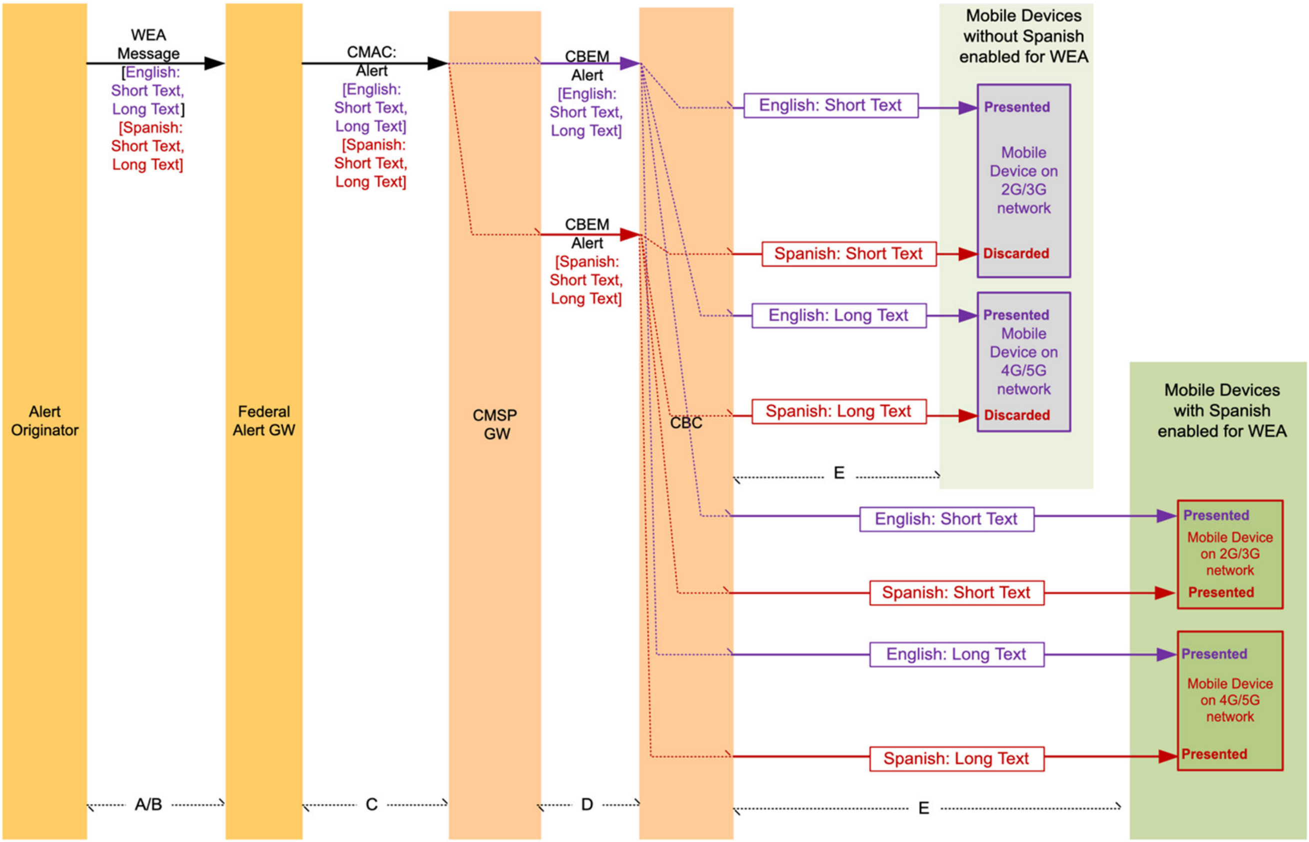

Alert Originator
WEA Message
[English: Short Text, Long Text]
[Spanish: Short Text, Long Text]
Federal Alert GW
CMAC: Alert
[English: Short Text, Long Text]
[Spanish: Short Text, Long Text]
CMSP GW
CBEM Alert
[English: Short Text, Long Text]
CBEM Alert
[Spanish: Short Text, Long Text]
CBC
Mobile Devices without Spanish enabled for WEA
English: Short Text
Presented
Mobile Device on 2G/3G network
Spanish: Short Text
Discarded
English: Long Text
Presented
Mobile Device on 4G/5G network
Spanish: Long Text
Discarded
E
Mobile Devices with Spanish enabled for WEA
English: Short Text
Presented
Mobile Device on 2G/3G network
Spanish: Short Text
Presented
English: Long Text
Presented
Mobile Device on 4G/5G network
Spanish: Long Text
Presented
A/B
C
D
E

Figure 6-3: Combined View of WEA Message Flow in Multiple Lengths and Languages

The Alert Originator sends a WEA message with short text (English and Spanish) and long text (English and Spanish) to the Federal Alert Gateway over the A/B interface.

The Federal Alert Gateway forwards a WEA message with short text (English and Spanish) and long text (English and Spanish) to the CMSP Gateway using the modified C interface.

The CMSP Gateway uses the English (with short text and long text) and Spanish (with short text and long text) WEA messages to create two independent alerts and sends one carrying the English alert text and one carrying the Spanish alert text over the D interface.

The CBC sends the WEA with short text toward mobile devices that receive messages over 2G/3G radio network and WEA with long text toward mobile devices that receive the WEA over 4G/5G radio network.

The mobile devices connected to the 2G/3G radio networks will receive the WEA messages with short text (English and Spanish, the latter when enabled). The English alert text will always be presented. If the mobile device user has Spanish enabled for WEA, the mobile device will also present the Spanish alert text.

NOTE: 4G/5G devices may also receive WEA over 2G/3G networks.

The mobile devices connected to the 4G/5G networks will receive the WEA messages in long text (English and Spanish, the later when enabled). The English alert text will always be presented. If the mobile device user has Spanish enabled for WEA, the mobile device will also present the Spanish alert text.

See flow in Figure 6-4 and

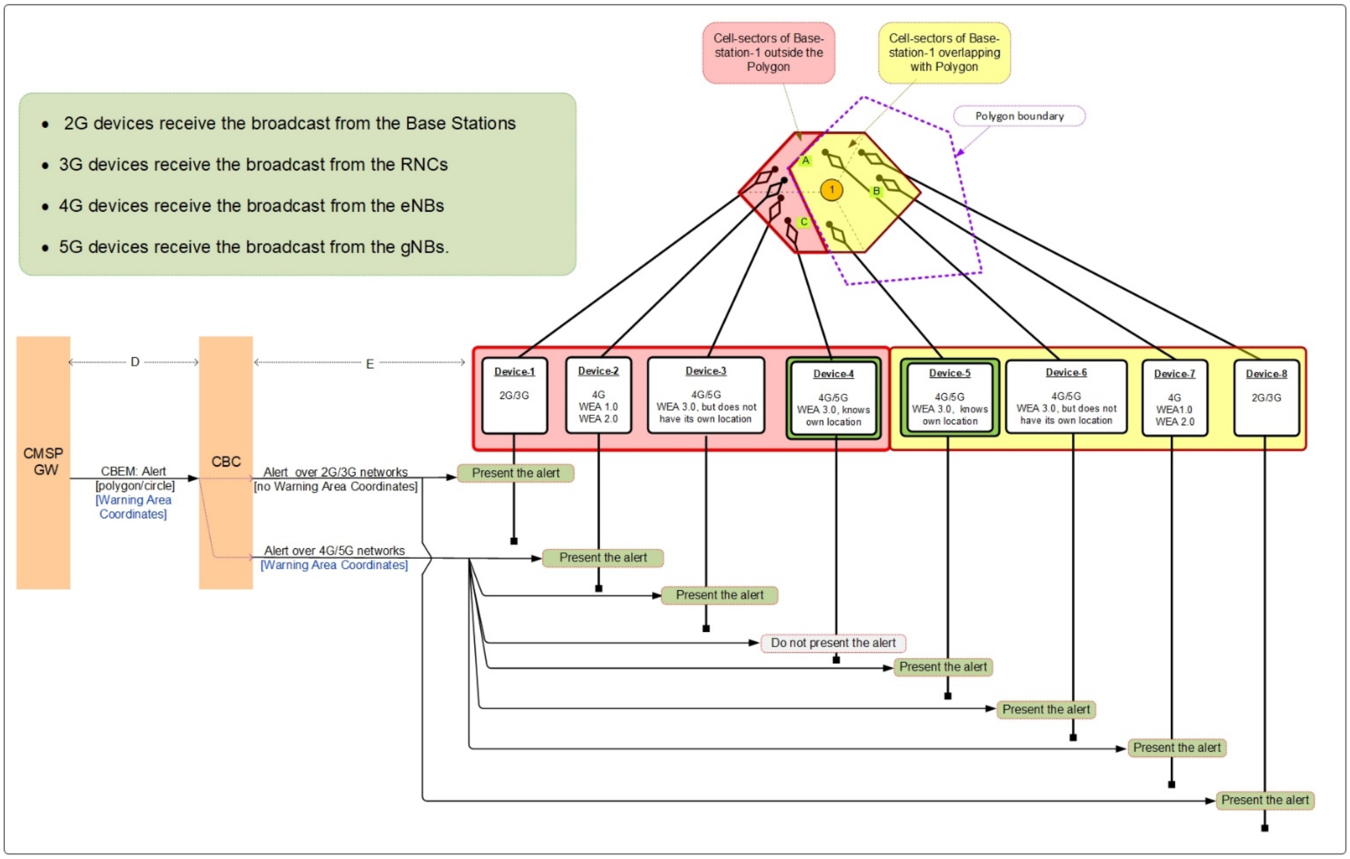

Cell-sectors of Base-station-1 outside the Polygon
Cell-sectors of Base-station-1 overlapping with Polygon
Polygon boundary
2G devices receive the broadcast from the Base Stations
3G devices receive the broadcast from the RNCs
4G devices receive the broadcast from the eNBs
5G devices receive the broadcast from the gNBs.
A
1
B
C
D
E
CMSP GW
CBC
CBEM: Alert [polygon/circle] [Warning Area Coordinates]
Alert over 2G/3G networks [no Warning Area Coordinates]
Alert over 4G/5G networks [Warning Area Coordinates]
Device-1 2G/3G
Device-2 4G WEA 1.0 WEA 2.0
Device-3 4G/5G WEA 3.0, but does not have its own location
Device-4 4G/5G WEA 3.0, knows own location
Device-5 4G/5G WEA 3.0, knows own location
Device-6 4G/5G WEA 3.0, but does not have its own location
Device-7 4G WEA1.0 WEA 2.0
Device-8 2G/3G
Present the alert
Present the alert
Present the alert
Do not present the alert
Present the alert
Present the alert
Present the alert
Present the alert

Figure 6-5 for the DBGF aspects of WEA.

6.2.4 Broadcast of Warning Area Coordinates

This clause presents the broadcast of WEA messages that include the Warning Area Coordinates which in turn provides the coordinates of polygons or circles representing the Alert Area. The Warning Area Coordinates are broadcast over 4G and later generation networks to enable DBGF in any WEA 3.0 capable device.

The Warning Area Coordinates are not included in the WEA broadcast to the mobile devices in the following cases:

- No coordinates were received from the Alert Originator because the Alert Area was only defined by one or more geocodes.
- Alert Originator includes the DBGF Bypass indicator.

The end-to-end view of WEA message flow without the Warning Area Coordinates are shown in Figure 6-1, Figure 6-2, and Figure 6-3.

An end-to-end view of WEA message flow with short text and long text in English and Spanish is as shown in Figure 6-3 is expanded in Figure 6-4 below to illustrate the transmission of Warning Area Coordinates.

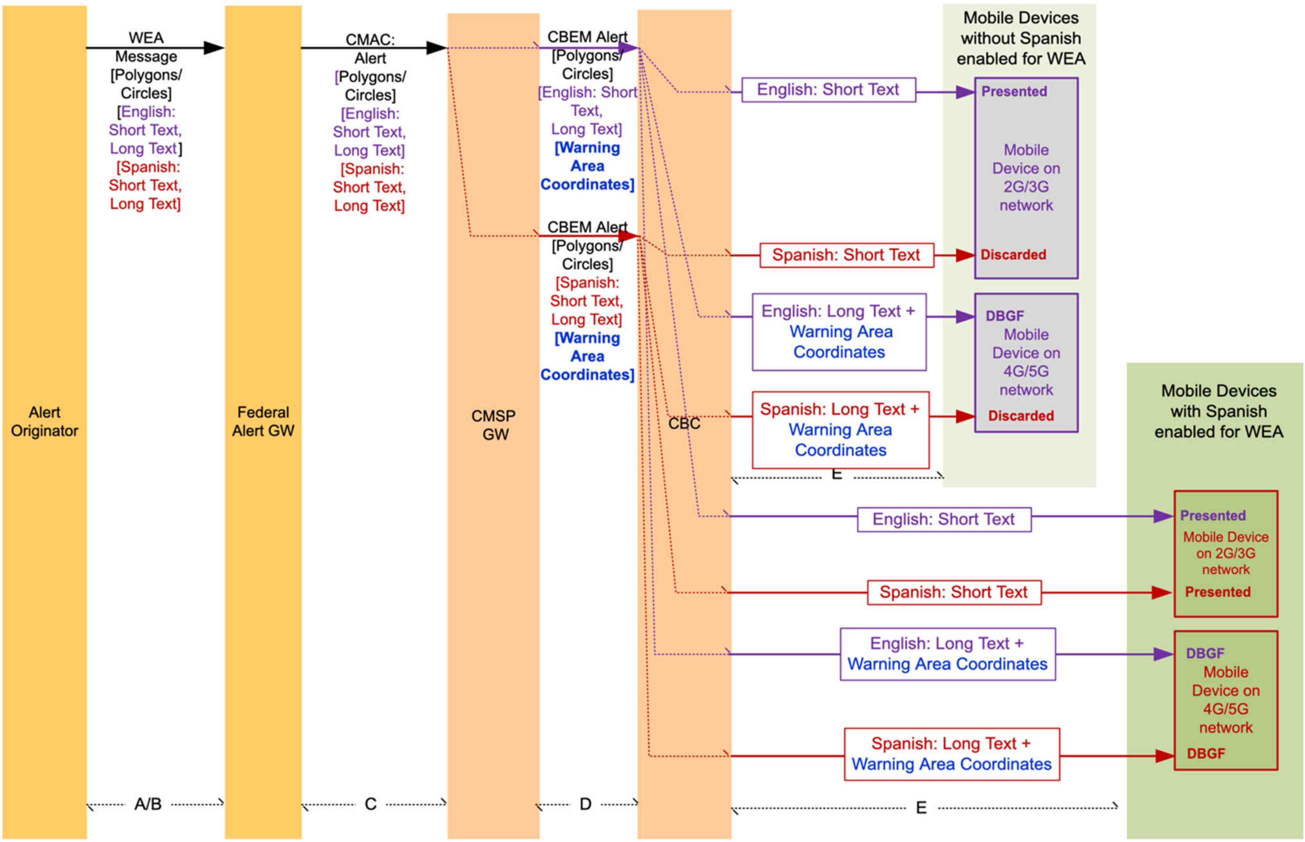

Alert Originator
WEA Message [Polygons/ Circles] [English: Short Text, Long Text] [Spanish: Short Text, Long Text]
Federal Alert GW
CMAC: Alert [Polygons/ Circles] [English: Short Text, Long Text] [Spanish: Short Text, Long Text]
CMSP GW
CBEM Alert [Polygons/ Circles] [English: Short Text, Long Text] [Warning Area Coordinates]
CBEM Alert [Polygons/ Circles] [Spanish: Short Text, Long Text] [Warning Area Coordinates]
CBC
Mobile Devices without Spanish enabled for WEA
English: Short Text
Presented
Mobile Device on 2G/3G network
Spanish: Short Text
Discarded
English: Long Text + Warning Area Coordinates
DBGF
Mobile Device on 4G/5G network
Spanish: Long Text + Warning Area Coordinates
Discarded
E
Mobile Devices with Spanish enabled for WEA
English: Short Text
Presented
Mobile Device on 2G/3G network
Spanish: Short Text
Presented
English: Long Text + Warning Area Coordinates
DBGF
Mobile Device on 4G/5G network
Spanish: Long Text + Warning Area Coordinates
DBGF
A/B
C
D
E

Figure 6-4: Combined View of WEA Message Flow in Multiple Lengths, Languages, and Warning Area Coordinates

The Alert Originator sends a WEA message that includes short text (English and Spanish) and long text (English and Spanish) to the Federal Alert Gateway over the A/B Reference Point. The geo-targeting information includes the polygons/circles. There is no indication from the Alert Originator to bypass the DBGF.

The Federal Alert Gateway forwards a WEA message that includes short text (English and Spanish) and long text (English and Spanish) to the CMSP Gateway using the modified C interface. The geo-targeting information includes the polygons/circles.

The CMSP Gateway uses the English (with short text and long text) and Spanish (with short text and long text) to create two independent alerts and sends each to the CBC separately over the D interface. The CMSP Gateway includes the Warning Area Coordinates in the broadcast for each alert.

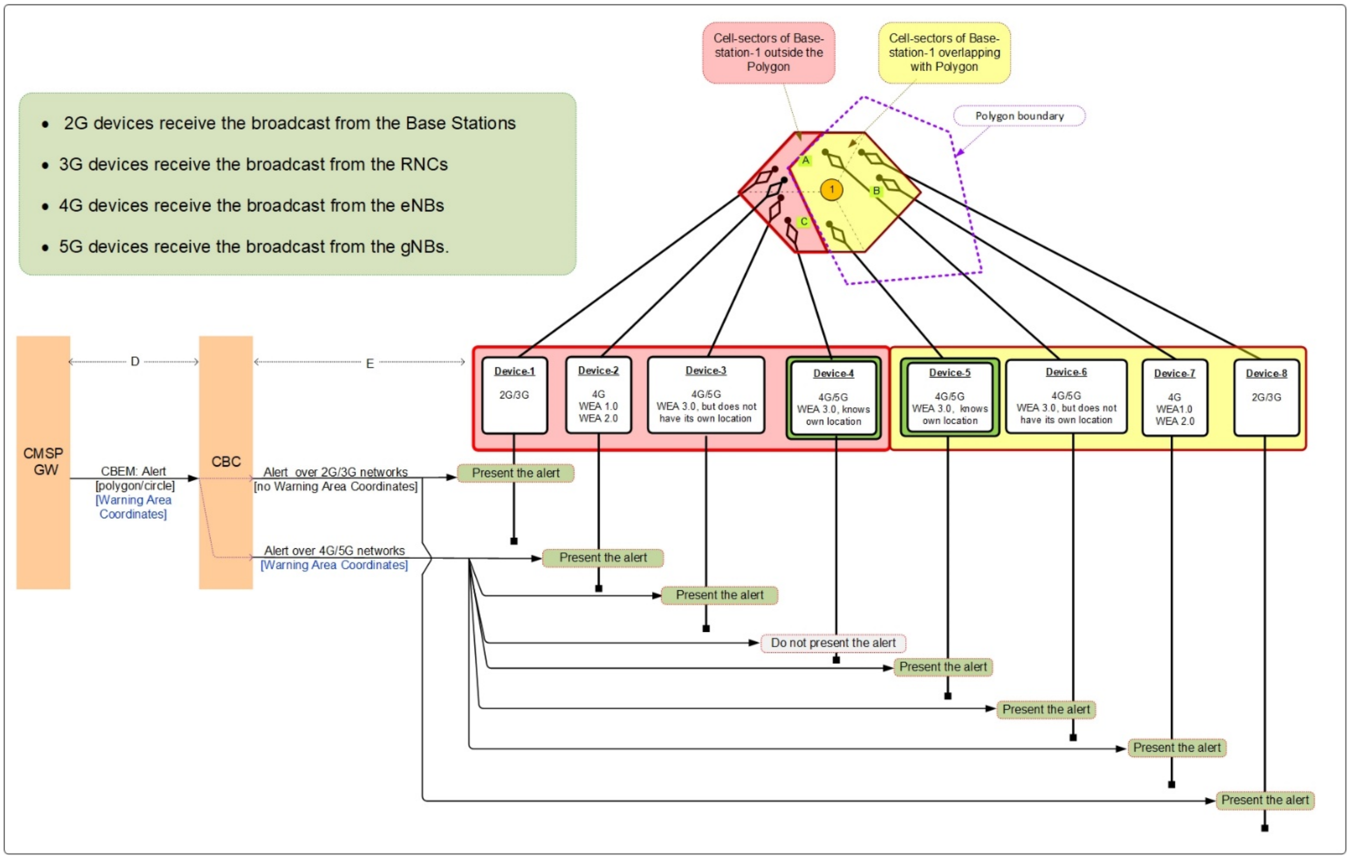
The CBC transmits the short text over the 2G/3G/4G/5G mobile devices as independent WEA messages over the E interface without the Warning Area Coordinates. The CBC sends the WEA messages with long text (English) and long text (Spanish) over the 4G/5G networks as independent WEA messages over the E interface with the Warning Area Coordinates.

The mobile devices connected to the 2G/3G networks will receive the WEA messages in short text (English and Spanish, the latter when enabled). The English alert text will always be presented. If the mobile device user has Spanish enabled for WEA, the mobile device will also present the Spanish alert text.

The mobile devices connected to the 4G/5G networks will receive the WEA messages in short text (English and Spanish, the latter when enabled). If, per the DBGF principles (see Clause 6.2.5), the alert is to be presented, the English alert text will always be presented. If the mobile device user has Spanish enabled for WEA, the mobile device will also present the Spanish alert text.

6.2.5 Device-Based Geo-Fencing at the mobile devices

This clause presents the handling of DBGF within the mobile devices when the received WEA message includes Warning Area Coordinates as shown in Figure 6-5 below.


Cell-sectors of Base-station-1 outside the Polygon
Cell-sectors of Base-station-1 overlapping with Polygon
Polygon boundary
2G devices receive the broadcast from the Base Stations
3G devices receive the broadcast from the RNCs
4G devices receive the broadcast from the eNBs
5G devices receive the broadcast from the gNBs.
A
B
C
1
D
E
CMSP GW
CBC
CBEM: Alert [polygon/circle] [Warning Area Coordinates]
Alert over 2G/3G networks [no Warning Area Coordinates]
Alert over 4G/5G networks [Warning Area Coordinates]
Device-1 2G/3G
Device-2 4G WEA 1.0 WEA 2.0
Device-3 4G/5G WEA 3.0, but does not have its own location
Device-4 4G/5G WEA 3.0, knows own location
Device-5 4G/5G WEA 3.0, knows own location
Device-6 4G/5G WEA 3.0, but does not have its own location
Device-7 4G WEA1.0 WEA 2.0
Device-8 2G/3G
Present the alert
Present the alert
Present the alert
Do not present the alert
Present the alert
Present the alert
Present the alert
Present the alert

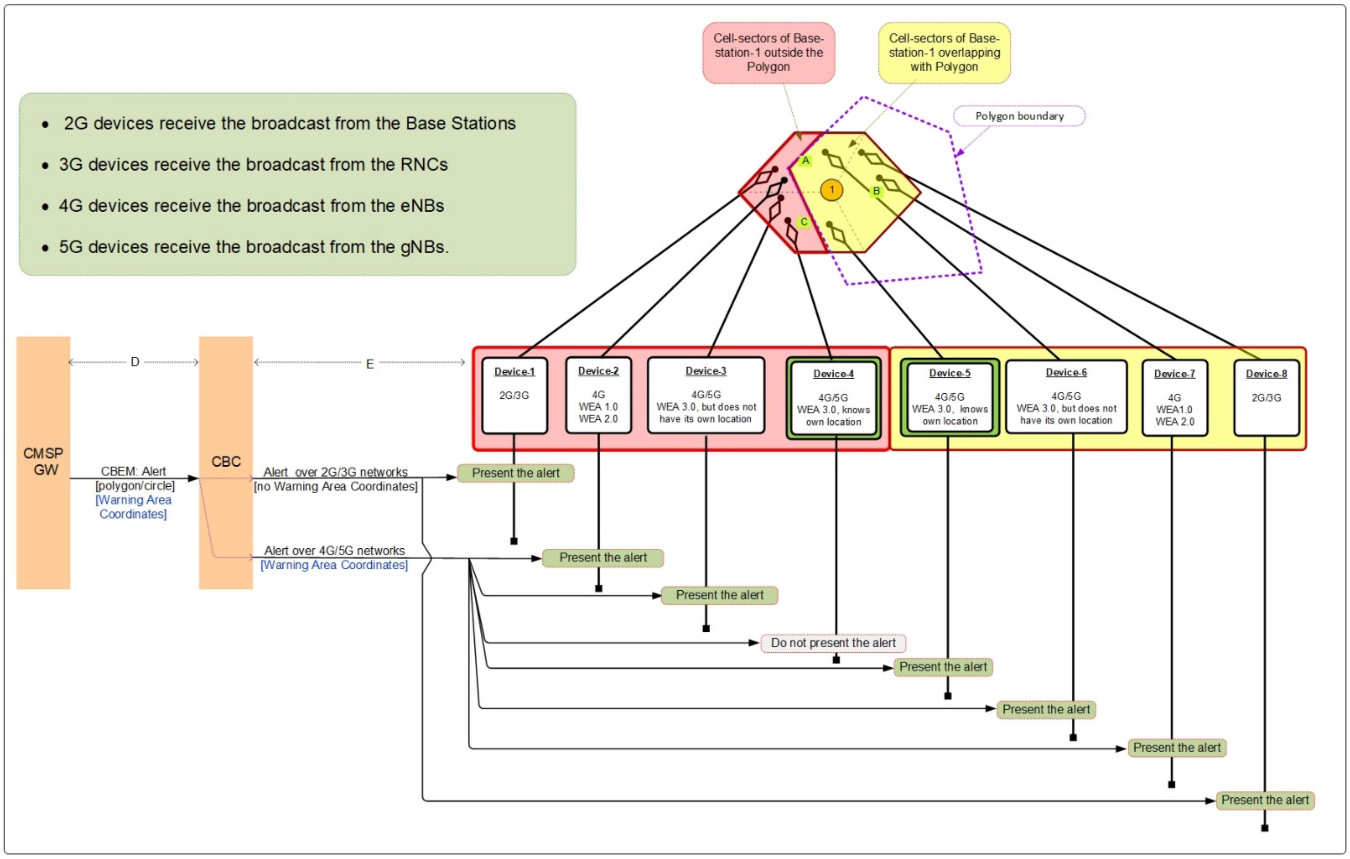

Cell-sectors of Base-station-1 outside the Polygon
Cell-sectors of Base-station-1 overlapping with Polygon
Polygon boundary
2G devices receive the broadcast from the Base Stations
3G devices receive the broadcast from the RNCs
4G devices receive the broadcast from the eNBs
5G devices receive the broadcast from the gNBs.
A
B
C
1
D
E
CMSP GW
CBC
CBEM: Alert [polygon/circle] [Warning Area Coordinates]
Alert over 2G/3G networks [no Warning Area Coordinates]
Alert over 4G/5G networks [Warning Area Coordinates]
Device-1 2G/3G
Device-2 4G WEA 1.0 WEA 2.0
Device-3 4G/5G WEA 3.0, but does not have its own location
Device-4 4G/5G WEA 3.0, knows own location
Device-5 4G/5G WEA 3.0, knows own location
Device-6 4G/5G WEA 3.0, but does not have its own location
Device-7 4G WEA1.0 WEA 2.0
Device-8 2G/3G
Present the alert
Present the alert
Present the alert
Do not present the alert
Present the alert
Present the alert
Present the alert
Present the alert

Figure 6-5: DBGF handling within the mobile devices

NOTE: The illustration shown in the

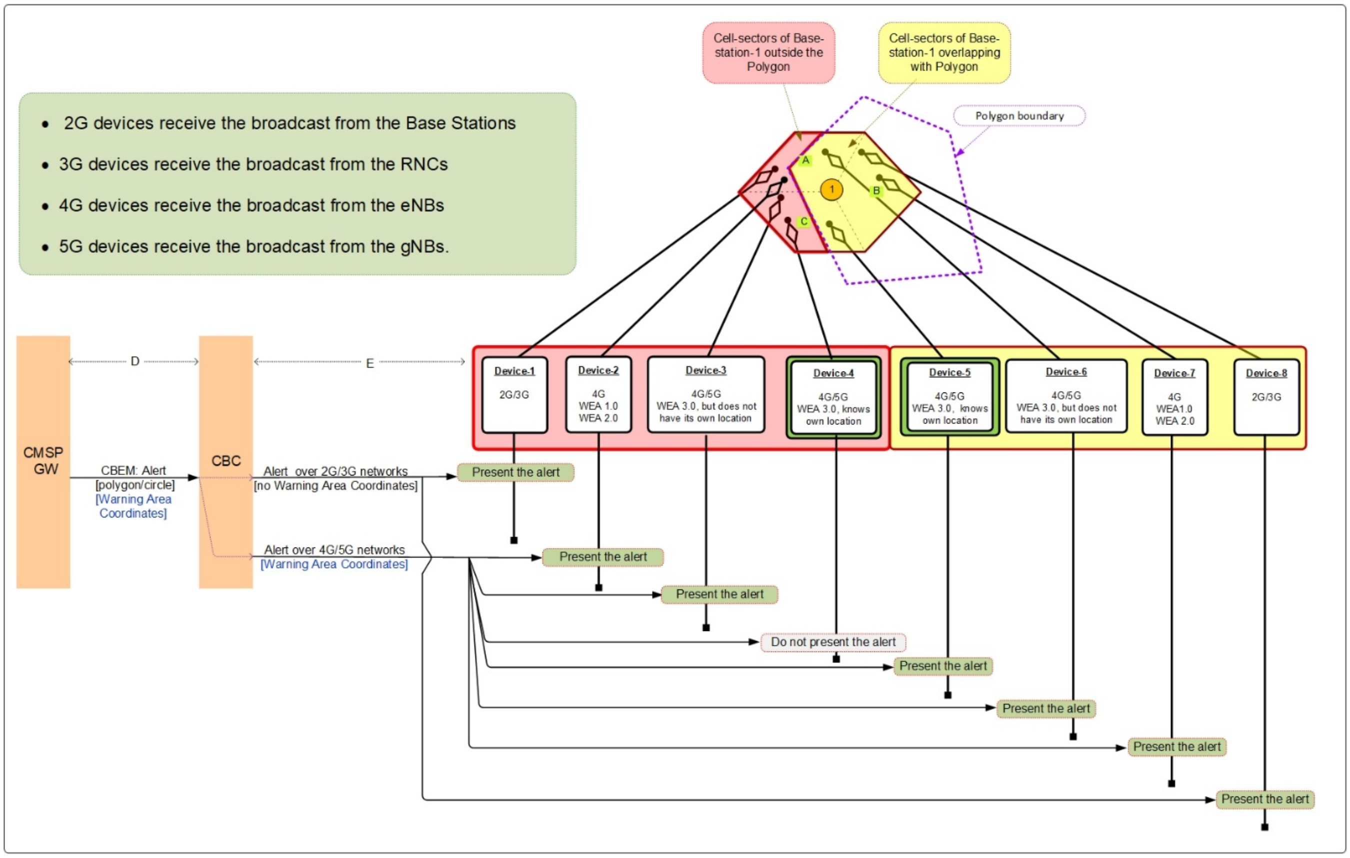
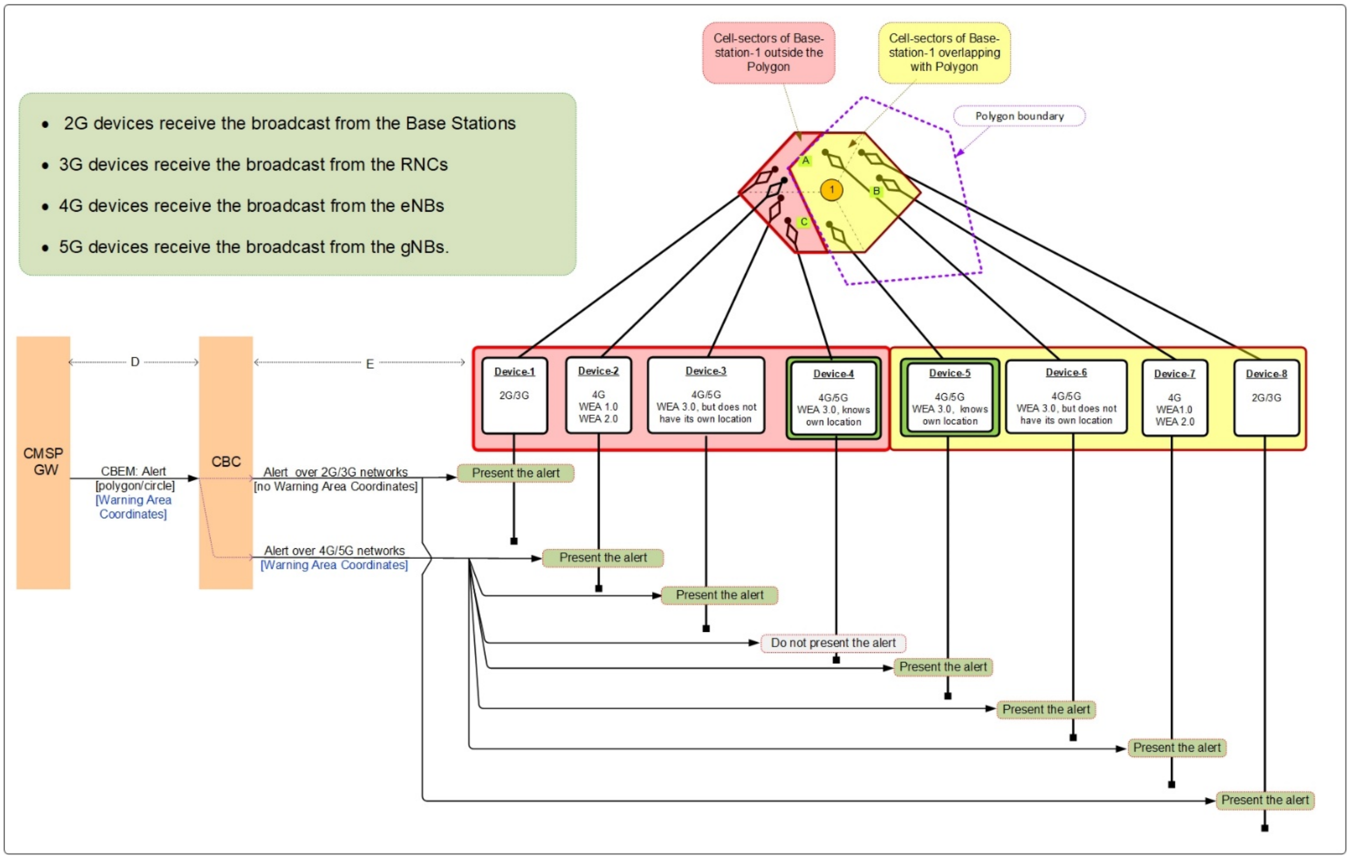

Cell-sectors of Base-station-1 outside the Polygon
Cell-sectors of Base-station-1 overlapping with Polygon
Polygon boundary
2G devices receive the broadcast from the Base Stations
3G devices receive the broadcast from the RNCs
4G devices receive the broadcast from the eNBs
5G devices receive the broadcast from the gNBs.
A
B
C
1
D
E
CMSP GW
CBC
CBEM: Alert [polygon/circle] [Warning Area Coordinates]
Alert over 2G/3G networks [no Warning Area Coordinates]
Alert over 4G/5G networks [Warning Area Coordinates]
Device-1 2G/3G
Device-2 4G WEA 1.0 WEA 2.0
Device-3 4G/5G WEA 3.0, but does not have its own location
Device-4 4G/5G WEA 3.0, knows own location
Device-5 4G/5G WEA 3.0, knows own location
Device-6 4G/5G WEA 3.0, but does not have its own location
Device-7 4G WEA1.0 WEA 2.0
Device-8 2G/3G
Present the alert
Present the alert
Present the alert
Do not present the alert
Present the alert
Present the alert
Present the alert
Present the alert

Figure 6-5 assumes that the received WEA message has been opted in within the mobile devices.


Cell-sectors of Base-station-1 outside the Polygon
Cell-sectors of Base-station-1 overlapping with Polygon
Polygon boundary
2G devices receive the broadcast from the Base Stations
3G devices receive the broadcast from the RNCs
4G devices receive the broadcast from the eNBs
5G devices receive the broadcast from the gNBs.
A
B
C
1
D
E
CMSP GW
CBC
CBEM: Alert [polygon/circle] [Warning Area Coordinates]
Alert over 2G/3G networks [no Warning Area Coordinates]
Alert over 4G/5G networks [Warning Area Coordinates]
Device-1 2G/3G
Device-2 4G WEA 1.0 WEA 2.0
Device-3 4G/5G WEA 3.0, but does not have its own location
Device-4 4G/5G WEA 3.0, knows own location
Device-5 4G/5G WEA 3.0, knows own location
Device-6 4G/5G WEA 3.0, but does not have its own location
Device-7 4G WEA1.0 WEA 2.0
Device-8 2G/3G
Present the alert
Present the alert
Present the alert
Do not present the alert
Present the alert
Present the alert
Present the alert
Present the alert

Device-Based Geo-Fencing is illustrated in Figure 6-5 using eight (8) mobile devices. As shown, Device-1, Device-2, Device-3, and Device-4 are outside the polygon represented by the Warning Area Coordinates, while Device-5, Device-6, Device-7 and Device-8 are within the Polygon represented by Warning Area Coordinates. The handling of the WEA message within those eight mobile devices is as follows:

1. Device-1 and Device-8 are 2G/3G devices that do not support DBGF. Therefore, both mobile devices present the alert.
2. Device-2 and Device-7 are 4G mobile devices that are not enhanced to support DBGF (e.g., WEA 1.0 and WEA 2.0 4G mobile devices). Therefore, both mobile devices present the alert.
3. Device-3, Device-4, Device-5 and Device-6 are enhanced mobile devices (i.e., WEA 3.0) and hence, can support the DBGF.
    a. Device-3 and Device-6 are not able to determine their own location within the CMSP-configurable time-limit and default to presenting the alert.
    b. Device-4 determines its own location and finds out that it is located outside the polygon represented by the received Warning Area Coordinates and hence, it does not present the alert. Device-4 may receive additional instructions from the network at a later time, while the alert is still active, to re-check its location. If the device has moved into the alert area polygon at that point, the alert will be presented.
    c. Device-5 determines its own location and finds out that is within the polygon represented by the received Warning Area Coordinates and presents the alert.

6.3 Alert Cancellation

When a Cancel message is sent from the Federal Alert Gateway to the CMSP Gateway via the C interface, the Cancel message will contain the identification of the Alert or Update message to be cancelled.

After the Cancel message has been received and validated by the CMSP Gateway, it will initiate the steps to stop the broadcast associated with the initial Alert or Update message referenced in the Cancel message. The broadcast will be stopped in all associated languages and length formats (i.e., 90 and 360 characters). For example, if the Alert message to be cancelled is broadcast in both English and Spanish, the Cancel message will discontinue the broadcast of both the English and the Spanish versions of the alert.

The CMSP infrastructure does not send any indication to mobile devices that the alert message being broadcast was cancelled. The CMSP infrastructure does not create and broadcast any text message indicating that the alert has been cancelled.

If the Alert Originators want the general public to know that the alert has been cancelled, the Alert Originators will have to send a new alert message with text content indicating the cancellation of the alert. The Alert Originators will need to provide this new alert message with the same geo-targeting information as the cancelled message so that the information about the cancelled alert is broadcast to the same geographic area. The mobile devices handle this new alert that contains the information about the cancelled message in the same manner as illustrated in the flow diagrams of Clause 6.2.

6.4 Public Safety Message

The Public Safety Message is a category of WEA alert messages which the FCC defined in the FCC Report & Order on WEA Enhancements, FCC 16-127 [Ref 1]. In FCC 16-127 [Ref 1], the FCC defines the Public Safety Message as “an essential public safety advisory that prescribes one or more actions likely to save lives and/or safeguard property.”

Per §10.400 of Annex A Final Rules of FCC 16-127 [Ref 1], a Public Safety Message may only be issued in connection with an Alert Message classified as a Presidential Alert, an Imminent Threat Alert, or a Child Abduction/AMBER Alert. There is no enforcement of this regulation by the CMSPs or the CMSP network infrastructure.

By default, mobile devices are to receive and present the Public Safety Message. However, the mobile device user has the capability to opt-out of the presentation of Public Safety Messages as described in ATIS-0700036, Wireless Emergency Alert (WEA) 3.0 Mobile Device Behavior (MDB) Specification [Ref 4].

The Public Safety Message is sent over the C interface as an Alert, Update, or Cancel message with the special handling element set to indicate that this C interface message is a Public Safety Message.

The end-to-end flow diagram for the broadcast of Public Safety Message is same as illustrated in the flow diagrams of Clause 6.2.

6.5 State/Local WEA Test

The State/Local WEA Test message is a category of WEA alert messages which the FCC defined in the FCC Report & Order on WEA Enhancements, FCC 16-127 [Ref 1]. The purpose of the State/Local WEA Test message is to support proficiency training by the state and local Alert Originators. The FCC Report & Order FCC 16-127 [Ref 1] recommends that the Alert Originator clearly indicate in the text content of the State/Local WEA Test message that this message is a test message.

Unlike most alert classes, mobile devices are configured by default to an opt-out state for the State/Local WEA Test. The mobile device user may opt-in to enable the presentation of State/Local WEA Test messages as described in ATIS-0700036 [Ref 4].

The State/Local WEA Test message is sent over the C interface as a Alert, Update, or Cancel message with the special handling element set to indicate that this C interface message is a State/Local WEA Test message instead of an actual WEA alert. The CMSPs will transmit State/Local WEA Test messages immediately upon receipt in a manner consistent with requirements for WEA Imminent Threat messages.

A CMSP may forego a State/Local WEA Test message if the State/Local WEA Test message is preempted by actual alert traffic or if an unforeseen condition in the CMSP infrastructure precludes distribution of the State/Local WEA Test message. The CMSP Gateway, upon receipt of a State/Local WEA Test message, may immediately inform the Federal Alert Gateway using an error response on the C interface that there is a condition which precludes distribution.

The end-to-end flow diagram for the broadcast of State/Local WEA Test is same as illustrated in the flow diagrams of Clause 6.2.

Annex A
(informative)

A WEA Resources

This informative annex lists various reports, standards, specifications, RFCs, regulations etc., as applicable to WEA and are not necessarily referenced within the main body of this standard.

The Annex groups the list as shown below:

US Statutes

FCC Regulations & Documents

WEA 1.0 Standards

NOTE: The WEA 1.0 standards are those standards which are applicable prior to the WEA changes from the September 2016 FCC WEA Enhancements Report & Order, FCC 16-127 [Ref 1].

WEA 2.0 Standards

NOTE: The WEA 2.0 standards are those standards which are applicable after the WEA changes from the September 2016 FCC WEA Enhancements Report & Order, FCC 16-127 [Ref 1].

WEA 3.0 Standards

NOTE: The WEA 3.0 standards are those standards which are applicable after the WEA changes from the January 2018 FCC Second Report and Order and Second Order on Reconsideration, FCC 18-4 [Ref 2].

ATIS WEA Feasibility Studies

3GPP Specifications

IETF RFCs

Federal Standards and Specifications

OASIS Standards

ISO/IEC Specifications

W3C Specifications

INCITS Standards

Articles, Presentations, & Research Papers

A.1 US Statutes

The US statutes are available from the U.S. Government Printing Office at < http://www.gpo.gov/ >.

WARN Act, Security and Accountability For Every Port Act of 2006 (SAFE Port Act), Pub.L. 109-347, Title VI-Commercial Mobile Service Alerts (WARN Act).

A.2 FCC Regulations & Documents

The FCC regulations and documents are available from the Federal Communications Commission at < http://www.fcc.gov/ >.

FCC 07-214; Federal Communications Commission Notice of Proposed Rulemaking in the Matter of the Commercial Mobile Alert System; December 14th, 2007.

FCC 07-287; Federal Communications Commission (FCC) Commercial Mobile Alert System (CMAS) Notice of Proposed Rulemaking (NPRM), Docket 07-287; December 14, 2007.

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

FCC 08-164, Federal Communications Commission Second Report and Order and Further Notice of Proposed Rulemaking In the Matter of The Commercial Mobile Alert System; July 8, 2008.

FCC 08-184, Federal Communications Commission Third Report and Order and Further Notice of Proposed Rulemaking In the Matter of The Commercial Mobile Alert System; August 7th, 2008.

FCC 08-166, Federal Communications Commission Order on Reconsideration and Erratum In the Matter of The Commercial Mobile Alert System; July 15, 2008.

FCC 13-280, Federal Communications Commission Order In the Matter of The Commercial Mobile Alert System; February 25, 2013.

NOTE: FCC 13-280 is the FCC Order changing Commercial Mobile Alert System (CMAS) to Wireless Emergency Alerts (WEA).

FCC 16-127, Federal Communications Commission Report and Order and Further Notice of Proposed Rulemaking In the Matter of Wireless Emergency Alerts Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System; September 29, 2016.

FCC 18-4, Federal Communications Commission Second Report and Order and Second Order on Reconsideration; January 30, 2018.

FCC 21-77, Federal Communications Commission Report and Order and Further Notice of Proposed Rulemaking In the Matter of Wireless Emergency Alerts Amendments of Part 11 of the Commission's Rules Regarding the Emergency Alert System; June 17, 2021.

FCC CSRIC IV Working Group 4, Geographic Targeting, Message Content and Character Limitation Subgroup Report, October 2014.

Title 47 United States Code (U.S.C.) Section 225, Telecommunications services for hearing-impaired and speech-impaired individuals.

A.3 WEA 1.0 Standards

The WEA 1.0 specifications are available from the Alliance for Telecommunications Industry Solutions (ATIS) at < http://www.atis.org >.

NOTE: The WEA 1.0 specifications are those specifications which are applicable prior to WEA architecture change from September 2016 FCC Report & Order, FCC 16-127 [Ref 1].

ATIS-0700006, CMAS via GSM/UMTS Cell Broadcast Service Specification.

ATIS-0700006.a, Supplement A to ATIS-0700006, CMAS via GSM/UMTS Cell Broadcast Service Specification.

ATIS-0700007, Implementation Guidelines and Best Practices for GSM/UMTS Cell Broadcast Service Specification.

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

ATIS-0700010, WEA via EPS Public Warning System Specification.

ATIS-0700010.a, Supplement A to ATIS-0700010, WEA via EPS Public Warning System Specification.

ATIS-0700012.v002, ATIS Implementation Guidelines for CMAS Supplemental Information Retrieval Revision 2.

ATIS-0700013, Implementation Guidelines for Mobile Device Support of Multi-Language CMAS.

ATIS-0700014.v002, ATIS Implementation Guidelines for CMSP Handling of CMAS Supplemental Information Broadcast Revision 2.

ATIS-0700022, CMAS Supplemental Information Retrieval Interface Testing Specification.

ATIS-0700025, CMAS International Roaming Specification.

ATIS-0700032, Supplement B of J-STD-100, Joint ATIS/TIA CMAS Mobile Device Behavior Specification.

ATIS-0700033, Supplement C of J-STD-101, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification.

ATIS-0700034, Supplement B of J-STD-102, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Test Specification.

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

J-STD-100.a, Supplement A to J-STD-100, Joint ATIS/TIA CMAS Mobile Device Behavior Specification.

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

J-STD-101.a, Supplement A to J-STD-101, Joint ATIS/TIA CMAS Alert Gateway to CMSP Gateway Interface Specification.

J-STD-101.b, Supplement B to J-STD-101, Joint ATIS/TIA CMAS Alert Gateway to CMSP Gateway Interface Specification.

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

J-STD-102.a, Supplement A to J-STD-102, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Test Specification.

A.4 WEA 2.0 Standards

The WEA 2.0 specifications are available from the Alliance for Telecommunications Industry Solutions (ATIS) at < http://www.atis.org >.

NOTE 1: The WEA 2.0 specifications are those specifications which are applicable to WEA architecture change from September 2016 FCC Report & Order, FCC 16-127 [Ref 1].

NOTE 2: The titles of the WEA 2.0 specifications refer to WEA 2.0 as Enhanced Wireless Emergency Alert (eWEA).

ATIS-0700006.v002, Enhanced Wireless Emergency Alert (eWEA) via GSM/UMTS Cell Broadcast Service Specification.

ATIS-0700010.v002, Enhanced Wireless Emergency Alert (eWEA) via EPS Public Warning System Specification.

ATIS-0700035, Enhanced Wireless Emergency Alert (eWEA) Service Description.

ATIS-0700036, Enhanced Wireless Emergency Alert (eWEA) Mobile Device Behavior (MDB) Specification (a revised version of J-STD-100).

ATIS-0700037, Enhanced Wireless Emergency Alert (eWEA) Federal Alert Gateway to CMSP Gateway Interface Specification (a revised version of J-STD-101).

ATIS-0700038, Enhanced Wireless Emergency Alert (eWEA) Federal Alert Gateway to CMSP Gateway Interface Test Specification (a revised version of J-STD-102).

A.5 WEA 3.0 Standards

The WEA 3.0 specifications are available from the Alliance for Telecommunications Industry Solutions (ATIS) at < http://www.atis.org >.

NOTE: The WEA 3.0 specifications are those specifications which are applicable to WEA architecture change from January 2018 FCC Report & Order, FCC 18-4 [Ref 2] and June 2022 FCC Report and Order and Further Notice of Rulemaking, FCC 21-77 [Ref 3].

ATIS-0700006.v003, Wireless Emergency Alert (WEA) 3.0 via GSM/UMTS Cell Broadcast Service Specification.

ATIS-0700010.v004, Wireless Emergency Alert (WEA) 3.0 via EPS Public Warning System Specification.

ATIS-0700025.v002, Wireless Emergency Alert (WEA) International Roaming Specification.

ATIS-0700035, Wireless Emergency Alert (WEA) Service Description.

ATIS-0700036.v003, Wireless Emergency Alert (WEA) 3.0 Mobile Device Behavior (MDB) Specification.

ATIS-0700037.v003, Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway to CMSP Gateway Interface Specification.

ATIS-0700038.v003, Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway to CMSP Gateway Interface Test Specification.

ATIS-0700041.v002, Wireless Emergency Alerts (WEA) 3.0: Device-Based Geo-Fencing.

ATIS-0700043, Wireless Emergency Alert (WEA) 3.0 via 5G Public Warning System Specification.

ATIS-0700045, CMSP Gateway to Cell Broadcast Center (CBC) Interface Specification.

ATIS-0700049, WEA 3.0 Practical Hints for Alert Originators.

ARIS-0700050, Wireless Emergency Alert (WEA) 3.0 Operational Considerations for Commercial Mobile Service Providers (CMSPs).

A.6 ATIS WEA Feasibility Studies

The ATIS WEA feasibility studies are available from the Alliance for Telecommunications Industry Solutions (ATIS) at < http://www.atis.org >.

ATIS-0700023, Feasibility Study for LTE WEA Message Length.

ATIS-0700026, Feasibility Study for WEA Supplemental Text.

ATIS-0700027, Feasibility Study for WEA Cell Broadcast Geo-Targeting.

A.7 3GPP Specifications

The 3GPP standards are available from the 3rd Generation Partnership Project (3GPP) at < http://www.3gpp.org/ >.

3GPP TS 22.268, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Public Warning System (PWS) Requirements.

3GPP TS 23.038, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Alphabets and language-specific information.

3GPP TS 23.041, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Technical realization of Cell Broadcast Service (CBS).

3GPP TS 25.324, 3rd Generation Partnership Project; 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Broadcast/Multicast Control (BMC).

3GPP TS 25.419, 3rd Generation Partnership Project; Technical Specification Group RAN; UTRAN Iu-BC Interface: Service Area Broadcast Protocol (SABP).

3GPP TR 25.925, 3rd Generation Partnership Project; 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Radio interface for broadcast/multicast service.

3GPP TS 29.168, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Cell Broadcast Centre interfaces with the Evolved Packet Core; Stage 3.

3GPP TS 29.518, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 5G System; Access and Mobility Management Services; Stage 3.

3GPP TS 36.331, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC); Protocol specification.

3GPP TS 38.331, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NR; Radio Resource Control (RRC) protocol specification.

3GPP TS 36.413, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP).

3GPP TS 38.413, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NG-RAN; NG Application Protocol (NGAP).

3GPP TS 44.012, 3rd Generation Partnership Project; 3rd Generation Partnership Project; Technical Specification Group GSM EDGE Radio Access Network; Short Message Service Cell Broadcast (SMSCB) support on the mobile radio interface.

3GPP TS 48.049, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Base Station Controller - Cell Broadcast Centre (BSC-CBC) interface specification; Cell Broadcast Service Protocol (CBSP).

A.8 IETF RFCs

The IETF RFCs are available from the Internet Engineering Task Force (IETF) at < http://www.ietf.org >.

IETF STD 5 (RFC 791), Internet Protocol (IPv4) Specification.

IETF STD 5 (RFC 792), Internet Control Message Protocol.

IETF RFC 793, Transmission Control Protocol.

IETF RFC 1122, Requirements for Internet Hosts -- Communication Layers.

IETF RFC 1738, Uniform Resource Locators (URL).

IETF RFC 2141, *URN Syntax*.

NOTE: IETF RFC 2141 is referenced by the WEA 1.0 standards in Annex A.3. IETF RFC 2141 has been superseded by IETF RFC 8141 which is referenced by the eWEA Standards in Annex A.4.

IETF RFC 2404, The Use of HMAC-SHA-1-96 within ESP and AH.

IETF RFC 2460, Internet Protocol, Version 6 (IPv6) Specification.

NOTE: IETF RFC 2460 is referenced by the WEA 1.0 standards in Annex A.3. IETF RFC 2460 has been superseded by IETF RFC 8200 which is referenced by the eWEA Standards in Annex A.4.

IETF RFC 2464, Transmission of IPv6 Packets over Ethernet Networks.

NOTE: IETF RFC 2464 is referenced by the WEA 1.0 standards in Annex A.3. IETF RFC 2464 is not referenced by the eWEA Standards in Annex A.4.

IETF RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

NOTE: IETF RFC 2560 is referenced by the WEA 1.0 standards in Annex A.3. IETF RFC 2560 has been superseded by IETF RFC 6960 which is referenced by the eWEA Standards in Annex A.4.

IETF RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1.

NOTE: IETF RFC 2616 is referenced by the WEA 1.0 standards in Annex A.3. IETF RFC 2616 has been superseded by IETF RFC 7230 and IETF RFC 7231 which are referenced by the eWEA Standards in Annex A.4.

IETF RFC 3275, (Extensible Markup Language) XML-Signature Syntax and Processing.

NOTE: IETF RFC 3275 is referenced by the WEA 1.0 standards in Annex A.3. IETF RFC 3275 has been superseded by W3C Recommendation, Extensible Markup Language (XML) 1.1 (Second Edition) which is referenced by the eWEA Standards in Annex A.4.

IETF RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1.

NOTE: IETF RFC 3447 is referenced by the WEA 1.0 standards in Annex A.3. IETF RFC 3447 has been superseded by IETF RFC 8017 which is referenced by the eWEA Standards in Annex A.4.

IETF RFC 3602, The AES-CBC Cipher Algorithm and Its Use with IPsec.

IETF RFC 3715, IPsec-Network Address Translation (NAT) Compatibility Requirements.

IETF RFC 3986, Uniform Resource Identifier (URI): Generic Syntax.

IETF RFC 4158, Internet X.509 Public Key Infrastructure: Certification Path Building.

IETF RFC 4291, IP Version 6 Addressing Architecture.

IETF RFC 4301, Security Architecture for the Internet Protocol.

IETF RFC 4303, IP Encapsulating Security Payload (ESP).

IETF RFC 4305, Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).

NOTE: IETF RFC 4305 is referenced by the WEA 1.0 standards in Annex A.3. IETF RFC 4305 has been superseded by IETF RFC 7321 which is referenced by the eWEA Standards in Annex A.4.

IETF RFC 4306, Internet Key Exchange (IKEv2) Protocol.

NOTE: IETF RFC 4306 is referenced by the WEA 1.0 standards in Annex A.3. IETF RFC 4306 has been superseded by IETF RFC 7296 which is referenced by the eWEA Standards in Annex A.4.

IETF RFC 4443, Internet Control Message Protocol Version 6 (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.

NOTE: IETF RFC 4443 is referenced by the WEA 1.0 standards in Annex A.3. IETF RFC 4443 is not referenced by the eWEA Standards in Annex A.4.

IETF RFC 4718, IKEv2 Clarifications and Implementation Guidelines.

IETF RFC 4868, Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPSec.

IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

IETF RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

IETF RFC 7230, Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing.

IETF RFC 7231, Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content.

IETF RFC 7296, Internet Key Exchange Protocol Version 2 (IKEv2) Protocol.

IETF 7321, Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).

IETF RFC 8017, PKCS #1: RSA Cryptography Specifications Version 2.2.

IETF RFC 8141, Uniform Resource Names (URNs).

IETF RFC 8200, Internet Protocol, Version 6 (IPv6) Specification.

A.9 Federal Standards and Specifications

The Federal Information Processing Standards and the NIST specifications are available from the National Institute of Technology and Standards (NIST) at < http://www.nist.gov/aes >. The National Weather Service documents are available from the National Weather Service at < http://www.weather.gov/ >.

Federal Information Processing Standards Publication 5-2, Codes for the Identification of the States, the District of Columbia and the Outlying Areas of the United States, and Associated Areas; National Institute of Standards and Technology (NIST).

NOTE: The Federal Information Processing Standards Publication 5-2 is referenced by the WEA 1.0 standards in Annex A.3. NIST has withdrawn Federal Information Processing Standards Publication 5-2. The INCITS 38-2009, Codes for the Identification of the States and Equivalent Areas within the United States, Puerto Rico, and the Insular Areas (see Annex A.12) is the replacement standard and is referenced by the WEA 2.0 Standards in Annex A.4.

Federal Information Processing Standards Publication 6-4, *Counties and Equivalent Entities of the United States, its Possessions and Associated Areas*; National Institute of Standards and Technology (NIST).

NOTE: The Federal Information Processing Standards Publication 6-4 is referenced by the WEA 1.0 standards in Annex A.3. NIST has withdrawn Federal Information Processing Standards Publication 6-4. The INCITS 31-2009, Codes for the Identification of Counties and Equivalent Areas of the United States, Puerto Rico, and the Insular Areas (see Annex A.12) is the replacement standard and is referenced by the WEA 2.0 Standards in Annex A.4.

Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*.

NOTE: The Federal Information Processing Standards Publication 140-2 is referenced by the WEA 1.0 standards in Annex A.3. The Federal Information Processing Standards Publication 140-2 is not referenced by the WEA 2.0 Standards in Annex A.4.

Federal Information Processing Standards Publication 180-3, *Secure Hash Standard*; National Institute of Standards and Technology (NIST).

NOTE: The Federal Information Processing Standards Publication 180-3 is referenced by the WEA 1.0 standards in Annex A.3. Federal Information Processing Standards Publication 180-3 is superseded by Federal Information Processing Standards Publication 180-4 which is referenced by the WEA 2.0 Standards in Annex A.4.

Federal Information Processing Standards Publication 180-4, Secure Hash Standard; National Institute of Standards and Technology (NIST).

National Weather Service Instruction 10-1712, Operations and Services Dissemination Policy NWSPD 10-17 NOAA Weather Radio (NWR) All Hazards Specific Area Message Encoding (SAME).

NIST SP 800-77, Guide to IPsec VPNs.

A.10 OASIS Standards

The OASIS standards are available from the Organization for the Advancement of Structured Information Standards (OASIS) at < http://www.oasis-open.org/specs/index.php >.

Common Alerting Protocol, v. 1.2; OASIS Standard CAP-V1.2.

A.11 ISO/IEC Specifications

The ISO/IEC specifications are available from the International Organization for Standardization (ISO) at < http://www.iso.org >.

ISO 6709:2008, Standard Representation of Geographic Point Location by Coordinates.

ISO/IEC 10646:2003, Information technology -- Universal Multiple-Octet Coded Character Set (UCS).

A.12 W3C Specifications

This W3C specification is available from the World Wide Web Consortium (W3C) at < http://www.w3.org/TR/xmldsig-core/ >.

W3C Recommendation, Exclusive XML Canonicalization Version 1.0.

W3C Recommendation, Extensible Markup Language (XML) 1.1 (Second Edition).

W3C Recommendation, Namespaces in XML 1.1 (Second Edition).

W3C Recommendation, XML Encryption Syntax and Processing.

W3C Recommendation, XML Schema Definition Language (XSD) 1.1 Part 1: Structures.

W3C Recommendation, XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes.

W3C Recommendation, XML Schema Part 0: Primer Second Edition.

W3C Recommendation, XML Signature Syntax and Processing, Version 1.1.

A.13 INCITS Standards

The INCITS Standards are developed by the International Committee for Information Technology Standards (INCITS) http://www.incits.org/.

INCITS 38-2009, Codes for the Identification of the States and Equivalent Areas within the United States, Puerto Rico, and the Insular Areas; International Committee for Information Technology Standards (INCITS).[3]

INCITS 31-2009, Codes for the Identification of Counties and Equivalent Areas of the United States, Puerto Rico, and the Insular Areas; International Committee for Information Technology Standards (INCITS).[4]

A.14 Articles, Presentations, & Research Papers

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

Michele Wood, Hamilton Bean, Brooke Liu & Marcus Boyd, DHS START, Comprehensive Testing of

[3] Available from the International Committee for Information Technology Standards (INCITS) at < https://standards.incits.org/apps/group_public/project/details.php?project_id=206 >.

[4] Available from the International Committee for Information Technology Standards (INCITS) at < https://standards.incits.org/apps/group_public/project/details.php?project_id=204 >.

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

Imminent Threat Public Messages for Mobile Devices: Updated Findings; August 2015.[6]

[6] Report available from DHS at:

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

Annex B
(informative)

B WEA Regulations

The information in this annex will allow the reader to compare the WEA regulations as applicable to WEA 1.0 with the WEA regulations as applicable to WEA 2.0 and WEA 3.0 to understand the scope and nature of the regulatory changes.

The reference information for the documents and specifications mentioned in the annex is available in *Annex A, WEA Resources.*

B.1 Legislative & Regulatory Background

The Warning Alert and Response Network (WARN) Act[7] is part of the Security and Accountability For Every Port Act of 2006 (SAFE Port Act) which was passed by Congress in September 2006 and was signed into law by President Bush on October 13, 2006.

Based upon the WARN Act, "*the Commission[8] shall complete a proceeding to adopt relevant technical standards, protocols, procedures, and other technical requirements based on the recommendations of such Advisory Committee[9] necessary to enable commercial mobile service alerting capability for commercial mobile service providers that voluntarily elect to transmit emergency alerts*".[10]

Within the WARN Act, Congress defined Commercial Mobile Service Providers (CMSPs) as "*any 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)))*."[11]

B.2 Key WARN Act Provisions

The following is a summary of provisions in the WARN Act. Note that not all provisions may be applicable to this Standard, but are listed here for completeness. The provisions stated below are taken from the WARN Act and the reader should assume that term "commercial mobile service operators" and "commercial mobile service licensee" are synonymous with the term "commercial mobile service provider (CMSP)".

1. Commercial mobile service operators may voluntarily elect to transmit emergency alerts.[12]
2. A commercial mobile service operator who elects to transmit emergency alerts agrees to do so in a manner consistent with the technical standards, protocols, procedures, and other technical requirements implemented by the Commission.[13]
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.[14]

   NOTE: The Commercial Mobile Service Alert Advisory Committee (CMSAAC) interpreted the definition of "in whole or in part" to be "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".

4. A commercial mobile service operator who elects in whole or in part NOT to transmit emergency alerts:

[7] Security and Accountability For Every Port Act of 2006 (SAFE Port Act), Pub.L. 109-347, Title VI-Commercial Mobile Service Alerts (WARN Act)

[8] The "Commission" referenced in the WARN Act is the Federal Communications Commission.

[9] The "Advisory Committee" referenced in this quote is the Commercial Mobile Service Alerts Advisory Committee (CMSAAC) as in WARN Act § 602(a).

[10] WARN Act § 602(a)

[11] WARN Act § 602(b)(1)(A)

[12] WARN Act § 602(a)

[13] WARN Act § 602(b)(2)(B)(ii)

[14] WARN Act § 602(b)(1)(B)

   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.[15]

   b. Must provide notification of this decision to its existing subscribers.[16]

   c. Shall not by itself provide a basis for liability against the provider (including its officers, directors, employees, vendors, and agents).[17]

5. Commercial mobile service licensee may not impose a separate or additional charge for such transmission or capability.[18]

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.[19]

   a. Based upon the above WARN Act provision, the CMAS is considered to be an opt-out by the subscribers with the initial default configuration being that all emergency alerts are enabled.

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.[20]

   NOTE: The FCC First Report and Order, FCC 08-099, specifies CMAS alerts to be in English only.

8. Any commercial mobile service provider that transmits emergency alerts and meets it obligations 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.[21]

   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.[22]

B.3 FCC First Report and Order

The FCC released the First Report and Order for the Commercial Mobile Alert System, FCC 08-099, on April 9, 2008. This First Report and Order adopts the rules necessary to enable CMS alerting capability for CMS Providers who elect to transmit emergency alerts to their subscribers, adopted the architecture for the CMAS (see Clause B.7 *Reference Diagram*), and concluded that a Federal Government entity should aggregate, authenticate, and transmit alerts over the Reference Point C interface to the CMS Providers.

In addition, the First Report and Order adopts technologically neutral rules governing:

CMS Provider-controlled elements within the CMAS architecture (e.g., the CMS Provider Gateway, CMS Provider infrastructure and mobile devices).

Emergency alert formatting, classes, and elements: Participating CMS Providers must transmit three classes of alerts – Presidential, Imminent Threat, and AMBER alerts.

Geographic targeting (geo-targeting)**:** Participating CMS Providers generally are required to target alerts at the county-level as recommended by the CMSAAC.

Accessibility for people with disabilities and the elderly**:** Participating CMS Providers must include an audio attention signal and vibration cadence on CMAS-capable handsets.

[15] WARN Act § 602(b)(1)(B)

[16] WARN Act § 602(b)(1)(C)

[17] WARN Act § 602(e)(2)

[18] WARN Act § 602(b)(2)(C)

[19] WARN Act § 602(b)(2)(E) and § 603(c)(5)

[20] WARN Act § 602(c)(4)

[21] WARN Act § 602(e)(1)(A)

[22] WARN Act § 602(e)(1)(B)

Multi-language Alerting: Participating CMS Providers will not be required at this time to transmit alerts in languages other than English.

Availability of CMAS alerts while roaming: Subscribers receiving services pursuant to a roaming agreement will receive alert messages on the roamed upon network if the operator of the roamed upon network is a Participating CMS Provider and the subscriber's mobile device is configured for and technically capable of receiving alert messages from the roamed upon network.

Preemption of calls in progress: CMAS alerts may not preempt a voice or data session in progress.

Initial implementation: Participating CMS Providers must comply with these rules no later than 10 months from the date the FCC announces the selection of a Federal Government entity to perform the Alert Aggregator and Federal Alert Gateway functions required to implement the CMAS.

The First Report and Order FCC 08-99 specifies rules governing those sections of the CMAS architecture that are within the control of electing CMS Providers. These include the CMS Provider Gateway, CMS Provider infrastructure, and CMS Provider handsets. The rules require each individual CMS Provider Gateway to be able to receive alerts from the Federal Alert Gateway over a secure interface (i.e., Reference Point C Interface).

NOTE: On July 14, 2008, the FCC issued an Order on Reconsideration and Erratum dealing with CMAS timelines, which is beyond the scope of this Standard.

B.4 FCC Second Report and Order

The FCC released the Second Report and Order for the Commercial Mobile Alert System, FCC 08-164, on July 8, 2008. In the Second Report and Order, the FCC developed rules to be in compliance with section 602(c) of the WARN Act, which require non-commercial educational (NCE) and public broadcast television station licensees and permittees "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." (*Reference Point C Interface via Digital Television Transmission Towers*). Such equipment and technologies must have the capability of allowing licensees and permittees of NCE and public broadcast television stations to receive WEA alerts from the Alert Gateway over an alternate, secure interface and then to transmit such WEA alerts to CMS Provider Gateways of participating CMS providers."

The FCC Rules developed as a result of the Second Report and Order are contained in the Code of Federal Regulations (CFR), Title 47 – Telecommunications, Part 10 – Commercial Mobile Alert system, Subpart C – System Architecture, Section 10.340, Digital television transmission towers retransmission capability:

> Licensees and permittees of noncommercial educational broadcast television stations (NCE) or public broadcast television stations (to the extent such stations fall within the scope of those terms as defined in section 397(6) of the Communications Act of 1934 (47 U.S.C. 397(6))) are required to install on, or as part of, any broadcast television digital signal transmitter, equipment to enable the distribution of geographically targeted alerts by commercial mobile service providers that have elected to transmit WEA alerts. Such equipment and technologies must have the capability of allowing licensees and permittees of NCE and public broadcast television stations to receive WEA alerts from the Alert Gateway over an alternate, secure interface and then to transmit such WEA alerts to CMS Provider Gateways of participating CMS providers. This equipment must be installed no later than eighteen months from the date of receipt of funding permitted under section 606(b) of the WARN Act or 18 months from the effective date of these rules, whichever is later.

The FCC rules do not require a participating CMSP to support receiving alerts via digital television transmitters.

The National Telecommunications and Information Administration (NTIA) issued PBS a grant to install the 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. PBS manages the national public television interconnection system of non-commercial television stations that will support the WARN Act requirements.

The Second Report and Order also defines rules to implement section 602(f) of the WARN Act, which requires "technical testing for commercial mobile service providers that elect to transmit emergency alerts and for the devices and equipment used by such providers for transmitting such alerts". This technical testing is defined by the FCC rules to be a "Required Monthly Test" and "Periodic Interface Testing".

The Required Monthly Test (RMT) is initiated by the Federal Alert Gateway Administrator, and defines rules for the CMSP to schedule the distribution of the RMT to their CMAS coverage area over a 24-hour period commencing upon receipt of the RMT at the CMSP Gateway. A CMSP may provide mobile devices with the capability of receiving RMT messages.

A Participating CMS Provider may provide mobile devices with the capability of receiving Required Monthly Test (RMT) messages. The FCC does not require that CMS providers make available mobile devices that support reception of the required monthly test. The FCC does, however, allow CMS providers to choose to do so. CMS providers that choose not to make the required monthly test available to subscribers must find alternate methods of ensuring that subscriber handsets will be able to receive WEA alert messages. These alternative methods are beyond the scope of these standards.

The Periodic Interface Testing is a test message between the Federal Alert Gateway and the CMSP Gateway, and is intended to ensure the availability/viability of both gateway functions. The Periodic Interface Test is not designed to test the CMSP's infrastructure nor the mobile devices. The CMSP Gateway shall send an acknowledgement to the Federal Alert Gateway upon receipt of such an interface test message. The Periodic Interface Test is implemented as the Link Test Message.

B.5 FCC Third Report and Order

The FCC released the Third Report and Order for the Commercial Mobile Alert System, FCC 08-184, on August 7, 2008. In the Third Report and Order, the FCC adopted rules implementing Section 602(b) of the WARN Act. Specifically, the Third Report and Order adopts:

Notification requirements for CMS Providers that elect not to participate, or to participate only in part, with respect to new and existing subscribers;

Procedures by which CMS Providers may elect to transmit emergency alerts and to withdraw such elections;

A rule governing the provision of alert opt-out capabilities for subscribers; and

A compliance timeline under which participating CMS Providers must begin CMAS deployment.

The rule governing the provision of alert opt-out capabilities for subscribers specifies:

CMS Providers may provide their subscribers with the option to opt out of both, or either, the "Child Abduction Emergency/AMBER Alert" and "Imminent Threat Alert" classes of Alert Messages.

CMS Providers shall provide their subscribers with a clear indication of what each option means, and provide examples of the types of messages the customer may not receive as a result of opting-out.

Requirements and specifications for the subscribers' right to opt out as defined in the Third Report and Order may be found in the J-STD-100 *Joint ATIS/TIA CMAS Mobile Device Behavior Specification* and its associated Supplement A.

B.6 FCC Order to Rename CMAS to WEA

The authority-to-individual emergency alerting capability to mobile devices was originally called Commercial Mobile Alert System (CMAS) in the first three Reports and Orders from the FCC. The ATIS and the Joint ATIS/TIA standards were originally developed based upon the CMAS terminology and CMAS was operation in April 2012. However, in February 2013, the FCC renamed Commercial Mobile Alert System (CMAS) to Wireless Emergency Alerts (WEA) with associated updates to the appropriate sections of Part 11 of the 47 CFR. However, the ATIS and Joint ATIS/TIA standards were not retrofitted from CMAS to WEA and the message names, message elements, etc. retain the CMAS terminology.

B.7 FCC Report and Order on WEA Enhancements

On September 29, 2016, the FCC issued the FCC Report & Order on WEA enhancements, FCC 16-127 [Ref 1]. The WEA capabilities with these enhancements are referred to as WEA 2.0. Listed below are the WEA enhancements which are applicable to the support of WEA 2.0 via the GSM/UMTS Public Warning System (PWS).

Increasing Maximum WEA Character Length: Alert text increased to a maximum of 360 characters of alphanumeric on 4G-LTE and future networks. Allowed to continue the delivery of 90-character messages on 2G & 3G networks and devices.

- *Spanish-language Alerting*: Participating CMS Providers are required to transmit WEA Alert Messages that are issued in the Spanish language or that contain Spanish-language characters.
- *State/Local WEA Tests*: A Participating CMS Provider must support State/Local WEA Tests.
    1) A Participating CMS Provider's Gateway shall support the ability to receive a State/Local WEA Test message.
    2) A Participating CMS Provider shall immediately transmit a State/Local WEA Test to the geographic area specified by the alert originator.
    3) A Participating CMS Provider may forego a State/Local WEA Test if the State/Local WEA Test is pre-empted by actual alert traffic, or if an unforeseen condition in the CMS Provider infrastructure precludes distribution of the State/Local WEA Test. If a Participating CMS Provider Gateway forgoes a State/Local WEA Test, it shall send a response code to the Federal Alert Gateway indicating the reason.
    4) Participating CMS Providers shall provide their subscribers with the option to opt in to receive State/Local WEA Tests.
- A CMS Provider may not forego or delay delivery of a State/Local WEA Test message except when the test is preempted by actual Alert message traffic, or if an unforeseen condition in the Participating CMS Provider infrastructure precludes distribution of the State/Local WEA Test.
- *Classifying Public Safety Messages*: Public Safety Message is defined as “an essential public safety advisory that prescribes one or more actions likely to save lives and/or safeguard property”. Public Safety Messages will only be eligible for issuance in connection with an Imminent Threat Alert, an AMBER Alert, or a Presidential Alert. Participating CMS Providers shall provide for their subscribers to receive Public Safety Messages, by default, and may provide their subscribers with the option to opt out of receiving Public Safety Messages if they decide that they no longer wish to receive them. Participating CMS Providers are not required to associate a unique attention signal or vibration cadence with Public Safety Messages.
- *Supporting Embedded References and Multimedia:* Participating CMS Providers must support the transmission of embedded URLs and phone numbers in WEA Alert Messages. This amendment removes restriction on embedded references specified in the FCC First Report & Order, FCC 08-099. The inclusion of multimedia in WEA Alert Messages is a topic of the Further Notice of Proposed Rulemaking (FNPRM) portion of the FCC 16-127 [Ref 1] and, therefore, is out of scope for the WEA Rev 2 standards.
- *WEA Presentation*: Mobile devices must present an Alert Message as soon as they receive it, but mobile device may not enable an Alert Message to preempt an active voice or data session. WEA-capable mobile devices engaged in active voice or data sessions on 2G & 3G networks may not be able to receive available Alert Messages until the active voice or data session concludes. If a mobile device receives a WEA Alert Message during an active voice or data session, the user may be given the option to control how the Alert Message is presented on the mobile device with respect to the use of the common vibration cadence and audio attention signal.
- *WEA Geo-Targeting*: Participating CMS Provider must transmit any Alert Message that is specified by a geocode, circle, or polygon to an area that best approximates the specified geocode, circle, or polygon. If, however, the Participating CMS Provider cannot broadcast the Alert Message to an area that best approximates the specified geocode, circle, or polygon, a Participating CMS Provider may transmit an Alert Message to an area not larger than the propagation area of a single transmission site.
- *C1 Connection Testing*: Periodic C interface testing must include the testing of its public television broadcast-based backup. Pursuant to this framework, FEMA would initiate a test of the broadcast-based C interface backup by sending a test message through that infrastructure to the CMS Provider Alert Gateway, which would respond by returning an acknowledgement of receipt of the test message to the FEMA Gateway.

B.8 FCC Order on Reconsideration

On November 1, 2017, the FCC issued the FCC Order on Reconsideration, FCC 17-143. The portion of this Order of Reconsideration that is applicable to this specification is the FCC position on clickable embedded references. In paragraph 9, the FCC states the following:

> “Mobile devices that support neither embedded references nor the software updates that would provide such capability will not be considered WEA capable.”

In footnote 7, the FCC defines embedded references as follows:

> “Embedded references are links that contain telephone numbers or Uniform Reference Locators (URLs) that permit the message recipient to dial the telephone numbers or visit the URLS by clicking on the link.”

B.9 FCC Second Report and Order and Second Order on Reconsideration

On January 30, 2018, the FCC issues the FCC Second Report and Order and Second Order on Reconsideration, FCC-18-4. Two parts of this Report and Order are applicable to WEA 3.0:

- In paragraph 6, the FCC states the following:

> "We require Participating CMS Providers to deliver Alert Messages to an area that matches the target area specified by alert originators […] We define “matching” the target area as delivering an Alert Message to 100 percent of the target area with no more than 0.1 of a mile overshoot."

- In paragraph 17, the FCC states the following:

> "We amend Section 10.500 of the WEA rules to state that WEA-capable mobile devices must preserve Alert Messages in a consumer-accessible format and location for at least 24 hours after the Alert Message is received on the subscriber’s mobile device, or until deleted by the subscriber."

B.10 FCC Report and Order and Further Notice of Proposed Rulemaking

On June 17, 2021, the FCC issues the Report and Order and Further Notice of Proposed Rulemaking, FCC 21-77 [Ref 3]. One part of FCC 21-77 is applicable to WEA 3.0:

In 10.11, item (b), the FCC states the following:

> "If a Participating CMS Provider’s network infrastructure would generate and display WEA headers with the text “Presidential Alert” to subscribers upon receipt of a National Alert, or include the text “Presidential Alert” in a mobile device’s settings menus, then by July 31, 2022, that Participating CMS Provider’s network infrastructure shall either generate and display WEA headers and menus with the text “National Alert,” or no longer display those headers and menu text to the subscriber. Network infrastructure that is technically incapable of meeting this requirement, such as situations in which legacy devices or networks cannot be updated to support header display changes, are exempt from this requirement."

In 10.320, item (3), the FCC states the following:

> "Prioritization. The CMS provider gateway must process an Alert Message on a first in-first out basis except for National Alerts, which must be processed before all non-National Alerts."

In 10.400, item (a), the FCC states the following:

> "National Alert. A National Alert is an alert issued by the President of the United States or the President’s authorized designee, or by the Administrator of FEMA. National Alerts may be either nationwide or regional in distribution."

In 10.410, the FCC states the following:

> "A Participating CMS Provider is required to transmit National Alerts upon receipt. National Alerts preempt all other Alert Messages. A Participating CMS Provider is required to transmit Imminent Threat Alerts, AMBER Alerts and Public Safety Messages on a first in-first out (FIFO) basis."

In 10.500, the item (f), the FCC states the following:

> "Presentation of alert content to the device, consistent with subscriber opt-out selections. National Alerts must always be presented."

In Appendix B, paragraph 3, the FCC states the following:

> "Specifically, the Commission amends its rules to (i) replace WEA’s existing Presidential Alert class with a National Alert class that would ensure that WEA-enabled mobile devices could not opt out of receiving WEA alerts issued by the President (or the President’s authorized designee) or by the Administrator of the

> Federal Emergency Management Agency (FEMA); (ii) require participating Commercial Mobile Service (CMS) providers that use WEA header displays that read “Presidential Alert” to change those alert headers to read “National Alert” or to remove such headers altogether".

In Appendix B, paragraph 34, the FCC states the following:

> "In the Order, the Commission adds a national alert category to WEA that WEA-enabled mobile device users cannot opt-out of receiving. The national alert category changes the name of the current Presidential Alerts category to National Alerts and includes alerts from both the President and the FEMA Administrator. Participating CMS providers that use WEA header displays and settings menus that currently display "Presidential Alert" will have to change the display to read "National Alert" or discontinue their voluntary use of WEA header displays."