May, 2014

WORKING GROUP 2
Testing Subgroup
Report

Table of Contents

Table of Figures

Table of Tables

1 Preamble

This document contains the report of the Testing Subgroup of the Communications Security Reliability and Interoperability (CSRIC) IV Working Group 2. This report is intended to be incorporated into the overall CSRIC report.

2 Introduction

2.1 Overview and Executive Summary

Within the organization of CSRIC Working Group 2, sub-working groups have been established. Currently, one sub-working group is analyzing geotargeting, message content and character limitations and the other is examining end-to-end Wireless Emergency Alert (WEA) [1] testing. This report comes from the WG-2 Subgroup looking at testing. In this document we examine requirements and standards related to WEA testing, which via the RMT is currently national in scope and does not directly involve the state/local emergency management stakeholders.

The WG-2 Subgroup recommends Alerting Authorities be allowed to conduct a Localized WEA Test to Opt-in Participants. The Subgroup agreed that this localized Opt-In test achieves the maximum objectives for testing possible for an acceptable level of risk.

In order to enable this testing , the WG-2 Testing Subgroup recommends that the FCC clarify that WEA end-to-end testing beyond the RMT is not precluded by any of its existing rules.

Additionally, the WG-2 Testing Subgroup recommends that the FCC confirm that Section 602(e) of the WARN Act covers testing. In particular, the FCC should work with Congress or through other legislative means to clarify that the Section 602(e) protections against liability afforded to commercial mobile service providers extend to any WEA testing as this is a vital/essential function associated with alert transmission.

2.1.1 Organization Chart

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

Table 1 : CSRIC Committee Structure

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

2.1.2 Working Group 2, Testing Sub Group Membership

Table 2: CSRIC Testing Sub-Working Group Team Members

Name	Organization
Tim Dunn, Co-Chair	T-Mobile US
Matt May, Co-Chair	Johnson County Kansas Emergency Management & Communications
Brian Josef	CTIA
Bill Anderson	Carnegie Mellon University
Shellie Blakeney	T-Mobile US
Brian Daly	AT&T
Mike Gerber	NOAA
Denis Gusty	Department of Homeland Security Science & Technology
Robert Hoever	National Center for Missing and Exploited Children
Mark Lucero	Department of Homeland Security - FEMA
Bill Tortoriello	US Cellular
Xiaomei Wang	Verizon Wireless
Ganesh Ramesh	TCS
Cedric Cox	Intrado
Keith Bhatia	TCS
Julia Tu	FCC
James Wiley	FCC
Farrokh Khatibi	ATIS (Qualcomm)
Larry Rybar	Verizon Wireless
Francisco Sanchez	Greater Harris County
John Davis	Sprint
Matthew Straeb	GSS/Alert FM

Name	Organization
Carly Tapp	National Center for Missing and Exploited Children
Peter Musgrove	ATIS (AT&T)
Nag Rao	NSN

2.2 Objective of CSRIC IV Working Group 2 Testing Subgroup

The WG-2, Testing Subgroup is tasked with examining the WEA Service to explore the various facets of the current testing paradigm with an eye toward developing an approach that would support an option for end-to-end testing. This Subgroup documents the existing testing requirements and considers the interests of the stakeholders involved, including alert originators, federal government entities, state/local government organizations and the commercial mobile service providers.

2.3 WEA Architecture Diagram from CMSAAC

In the CMSAAC report, a Functional Reference Model diagram was used to describe the WEA system from end to end. This reference model is shown in Figure 1.

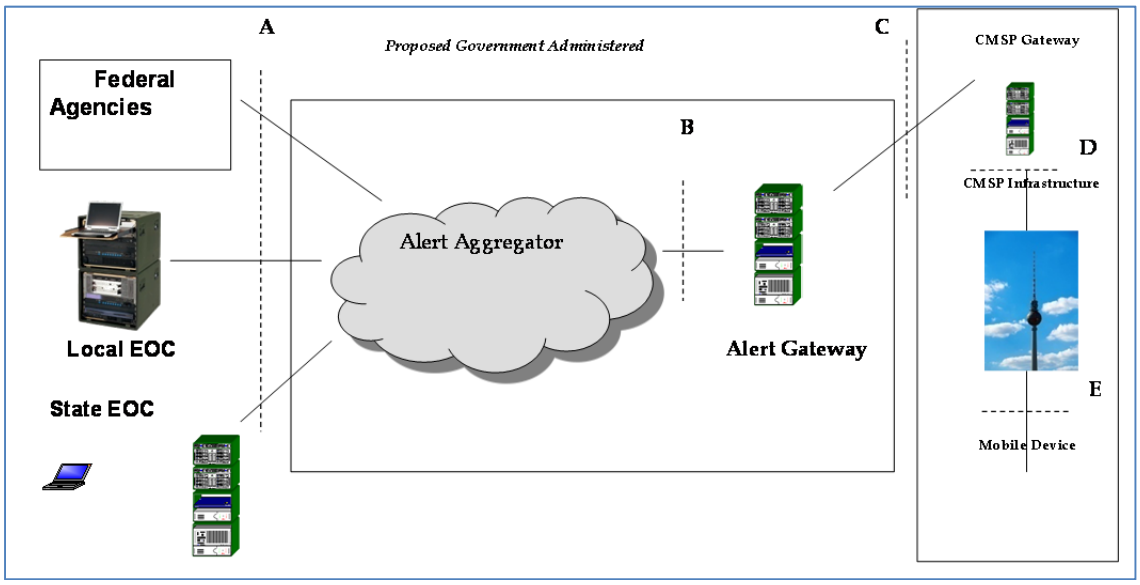


Figure 1 : CMSAAC WEA System Architecture

3 Analysis and Findings

3.1 Regulations & Statutes

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

Table 3: FCC Regulations and US Statutes

Number	Title	Description
FCC-07-214A1	FCC Notice of Proposed Rulemaking for Commercial Mobile Alert System	This is the FCC NPRM for CMAS. The results of the FCC Commercial Mobile Service Alert Advisory Committee (CMSAAC) are included in this NPRM.
FCC 08-099A1	FCC 1st Report and Order for Commercial Mobile Alert System	This is the FCC 1st Report and Order for Commercial Mobile Alert System. This FCC Report and Order contains the CMSAAC recommendations and defines the general CMAS functional requirements.
FCC 08-164A1	FCC 2nd Report and Order for Commercial Mobile Alert System	This is the FCC 2nd Report and Order for Commercial Mobile Alert System. This FCC Report and Order covers the Digital Television Transmission Towers Retransmission Capability and CMAS Testing Requirements.
FCC 08-184A1	FCC 3rd Report and Order for Commercial Mobile Alert System	This is the FCC 3rd Report and Order for Commercial Mobile Alert System. This FCC Report and Order covers the CMAS election procedures for CMSPs, CMAS withdrawal procedures for CMSPs, and subscriber notification requirements for CMAS.
WARN Act	Warning, Alert, and Response Network (WARN) Act	This is the statute that defined CMAS. The WARN Act is Title VI of H.R. 4954 "Security and Accountability For Every Port (SAFE) Act of 2006".
DA 13-280A1	Order in the Matter of the Commercial Mobile Alert System	The FCC revised Part 10 of its rules by changing the name "Commercial Mobile Alert System" to "Wireless Emergency Alerts" throughout the Part and by changing references from "CMAS" to "WEA."

3.2 Review of FCC CMSAAC Recommendations and FCC Rules on Testing

The WARN Act (Sec. 602, Paragraph (f), "Testing") states the Commission "…shall require by regulation technical testing…for the devices and equipment used…for transmitting such alerts."

A summary of the testing recommendations in the CMSAAC report are:

- Provision for testing of the CMAS, including the delivery mechanisms, without requiring all subscribers to see a test message.
- Provide the ability to send test messages to a single CMSP/network without impact to other CMSPs.
- Provide the ability to test the CMAS up to the CMSP Gateway without impacting the CMSP infrastructure.
- Provide CMSP access to the logs from the Alert Gateway.
- Messages used for testing purposes shall be clearly differentiated from messages for actual events.
- Provide for functional testing for the C Interface.
- Provide for Connection Testing of a new CMSP.
- Test each C-Interface Connection.
- Support keep-alive test messages periodically over the C interface.

The testing requirements codified in 47 C.F.R 10.350 as a result of the WARN Act and the CMSAAC Recommendations are summarized below.

- The Federal Alert Gateway Administrator shall send a Required Monthly Test to each CMSP that has elected to provide service. Each CMS Provider is required to support an RMT.
- CMSP's shall schedule the distribution of the RMT to their WEA coverage area over a 24 hour period that begins at the receipt of the RMT by the CMSP Gateway.
- CMSP's shall determine distribution method and may schedule the RMT over geographic subsets of their coverage area to manage traffic loads and accommodate maintenance windows.
- CMSP's shall distribute the RMT within 24 hours of receipt unless pre-empted by actual alert traffic or an inability to distribute the RMT due to an unforeseen condition.
- CMSP's may provide mobile devices with capability of receiving RMT messages.
- CMSP's must retain an automated log of RMT messages received.

3.3 Existing WEA Standards

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

3.4 Current Deployed Status of Testing

3.4.1 Current Monthly Testing Requirements

Section 602(f) of the WARN Act states that the Commission "shall require by regulation 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." In order to assure the reliability and performance of this new system, the Commercial Mobile Service Alert Advisory Committee ("CMSAAC") recommended certain procedures for logging WEA alerts at the Alert Gateway, and for testing the system at the Alert Gateway and testing on an end-to-end basis. End-to-end testing was defined by CMSAAC in 2007 as "testing from the Alert Initiator to the CMSP Gateway".

The Commission also agreed with the CMSAAC and most commenters that periodic testing of all components of the WEA, including the CMS provider's components would serve the public interest and is consistent with the WARN Act. Participating CMS providers must comply with these testing requirements no later than the date of deployment of WEA, which is the date that WEA development is complete and the WEA is functional and capable of providing alerts to the public. (See 47 C.F.R. § 10.350 - WEA Testing Requirements, summarized below.)

3.4.2 Summary and Constraints of existing RMT Process

Based on the CMAS Second Report and Order, the Required Monthly Test ("RMT") is initiated by the federally administered Alert Gateway at a set day and time and would be distributed through the commercial mobile service ("CMS") provider infrastructure and by participating CMS providers over their networks. Upon receipt of the test message, participating CMS providers would have a 24 hour window to distribute the test message in their WEA coverage areas in a manner that avoids congestion or other adverse effects on their networks. According to the ruling, the Federal Alert Gateway Administrator is to use a defined test message to distribute to the CMS provider's gateway. Use of real event codes and alert messages for tests are prohibited. CMS providers are to receive these required monthly test messages and must also distribute those test messages to their coverage area within 24 hours of receipt by the CMS Provider Gateway. CMS providers may determine how this delivery will be accomplished and may stagger the delivery of the required monthly test message over time and over geographic subsets of their coverage area to manage the traffic loads and accommodate maintenance windows. Participating CMS providers are to keep an automated log of RMT messages received by the CMS Provider Gateway from the Federal Alert Gateway. Additionally, a participating CMS provider may forego these monthly tests if preempted by actual alert traffic or in the event of unforeseen conditions in the CMS provider's infrastructure, but shall indicate this condition by a response code to the Federal Alert Gateway. CMS providers are not required to provide mobile devices that support reception of the required monthly test, yet are allowed to do so. However, CMS providers that choose not to make the RMT available to subscribers must find alternate methods of ensuring that subscriber handsets will be able to receive CMAS alert messages.[2]

Currently all participating CMS providers comply with the WEA test requirements conducted monthly by the Federal Alert Gateway Administrator. Each CMS provider connected across the C-Interface to the Federal Alert Gateway is sent the RMT message on the third Wednesday of every month at 1pm Eastern Time. Once the RMT message is received, the participating CMS Provider's Gateway routes the test message, within the 24-hour window based on CMS Provider's preference, to the wireless carrier's core infrastructure for further broadcast distribution out to the targeted network base-stations in the WEA coverage areas. Most CMS Providers have operational processes in place to receive the RMT on certain handsets which can be configured to receive the RMT message to avoid interrupting subscribers' handsets. The actual RMT message, from the Federal Alert Gateway, contains RMT special handling and event codes with a message that states, "This is a test of the Wireless Emergency Alert System. This is only a test". The RMT also contains 24-hour expiration from the origination date. Within the RMT operational process, the RMT messages are logged, along with active production alerts, on the CMSP Gateway, which stores the messages for an extended period of time.

3.4.3 Constraints of Network design, message identifiers, receipt and display of messages and other handset HMI issues

[2] *See* The Commercial Mobile Alert System, PS Docket No. 07-287, *Second Report and Order and Further Notice of Proposed Rulemaking*, 23 FCC Rcd 10765 (2008).

FEMA brought a redundant Federal Alert Gateway into operation in May 2013. Redundant gateways are necessary to improve system availability and to reduce single points of failure. The J-STD-101 supports redundant gateways and defines the message transmission requirements. Because redundant gateways are optional, each CMSP may employ a different network design to connect CMSP gateway(s) to the Federal Alert Gateways. Although the network designs are different, the message transmission arrangement, to include test messages, remains consistent regardless of network architecture.

Content of test messages could be impacted by changes in message length. As recent as Q1-2014, there has been a desire of some alert originators to exceed the 90 character limitation to provide a more meaningful message to the recipient. For further information on message length and content, please refer to the work of the Geographic Targeting, Message Content and Character Limitation sub-Working Group which is ongoing at the writing of this report.

Additionally, alert originators have requested different treatment with respect to vibration and tone, adding additional user configuration to the device on a per alert type basis. Currently WEA handset requirements are listed in J-STD-100, Joint ATIS/TIA CMAS Mobile Device Behavior Specification. This is an additional subject area that the CSRIC IV Working Group 2, among others, may study.

3.4.4 Link Test Messages

In addition to the required monthly test, periodic link test messages are sent on the "C" interface between the Federal Alert Gateway and each CMS Provider Gateway to ensure the availability of both gateway functions. The purpose of this periodic testing is to ensure that the Federal Alert Gateway is able to deliver WEA messages to the CMS Provider Gateway to ensure reliability of the WEA system. CMS Provider Gateways are to send an acknowledgement upon receipt of these interface test messages.

3.5 Requirements, Expectations and Outcomes of State and Local WEA Testing by Alert Originators

Alert Originators advise that training and exercises are a fundamental component of emergency management programs to ensure public safety. Testing the abilities of Alert Originators aids in proficiency for a real event, ensures the software used to generate WEA messages is operating correctly, and tests for downstream issues. Downstream issues can include problems with alert aggregation systems, the equipment/systems which broadcast the alerts, the recipient devices, and communication channels which connect all of the pieces. A failure in any of these can have broad implications which jeopardize public safety.

Emergency management officials on the Testing Sub Group put forth the following basic expectations and requirements for a true end to end test of WEA from Alert Originator to the recipient of the alert:

- This process would allow a test message, using a test message ID, to activate the system from Alert Originators to Alert Recipients in real time.
- In general, no more often than once a month.

- Could use a modified alerting tone (same audio just shorter) and/or modified alerting vibration cadence.
- No 24 hour hold window. Test alerts need to be sent immediately just as if they were non-test alert messages.
- Initiator controls the message content, not a single canned message.
- Could be an opt-out process for the tests only.
- Support would not be required from the carriers in the activation of the test.

3.5.1 Current Alert Testing

Some state and local jurisdictions conduct live code tests of EAS with broadcasters, emergency management agencies and NWS collaboration. This testing is often conducted in concert with seasonal preparedness campaigns (e.g., Severe Weather Awareness Week, Tsunami Preparedness Week, etc.) in order to maximize public awareness of the environmental hazard and understanding of the test. Awareness campaigns typically include participation by members of the media, such as local TV meteorologists, who share information with their viewers about upcoming tests as part of the campaign. The NWS maintains a Weather Preparedness Events Calendar at http://weather.gov/os/severeweather/severewxcal.shtml

Local Emergency Management offices currently test other notification systems for specific local hazards i.e. specific flash flood prone areas, nuclear power plants, and chemical storage facilities. These range from siren and loudspeaker systems to phone, email and text messaging systems. These notifications, like the natural hazards listed above, are part of a larger preparation campaign that is well known among the public likely to be impacted by including WEA in their existing testing process.

Large venue special events and key locations of national significance i.e. the Super Bowl, All Star baseball game, national monuments and other key locations are always potential targets where Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) weapons might be used. Preparing for CBRNE attacks could include utilizing WEA and educating the public by testing the system.

3.5.2 Amber Alert Testing

The National Center for Missing and Exploited Children does not have a requirement for routine testing of Amber Alerts.

3.5.3 FEMA Straw Poll of Alert Originators

An informal survey of Emergency Managers was initiated by FEMA/IPAWS on November 17, 2013, and asked questions related to the operation of localized alerting. The email questionnaire was sent to 226 organizations which had authority to send WEA messages at that time. FEMA/IPAWS received 62 responses, a summary of which are contained in the table 4 below:

Table 4 : FEMA/IPAWS Survey Summary

Question	Answer 1	Answer 2	Answer 3	Answer 4	Answer 5	Answer 6
Why is a WEA Test Code or testing capability Needed	A Test Code is needed (51)	A Test Code is NOT needed (1)	A silent test code is needed, but a live test code is not (10)			
Testing should be allowed for…	System Verification (45)	Maintain Operator Proficiency (25)	Public Awareness (11)	Accreditation Requirement (3)		
Testing should NOT be allowed because of	Public Opt Out/Alert Fatigue (4)					
How often would you exercise a "Silent" WEA test	Monthly (34)	Weekly (14)	Quarterly (6)	Semiannually (2)	Twice/Month (1)	Every 2 months (1) Never (1)
How often would you exercise a "Public" WEA Test	Annually (20)	Never (11)	Monthly (9)	Quarterly (9)	Semiannually (8)	Weekly (1) Every 2 Months (1)

3.5.4 Recommendations for Internal Testing of Existing WEA Operations

A summary of recommendations for testing were published in SEI Special Report – "Best Practices in Wireless Emergency Alerts", Mcgregor et al., CMU/SEI-2013-SR-015[3]. The following text in italics is extracted from that report:

To ensure that your office and your staff are ready and able to issue WEA messages, you should test your WEA system and procedures. Federal regulations do not permit the issuance of WEA messages for test purposes by any authority other than FEMA, so you cannot perform end-to-end testing in which test alerts are disseminated all the way to the public. Instead, you should plan and perform testing internal to your organization, using the JITC Test Lab provided by FEMA. The Test Lab is an instantiation of IPAWS-OPEN in a configuration that is consistent with the production version of IPAWS-OPEN but is not connected to any CMSPs. As such, it duplicates the functions of IPAWS-OPEN, without the possibility of sending an actual alert to the public. Its purpose is to provide AOs with the ability to test their systems and practice their skills in an environment without the risk of inadvertently issuing a "practice" alert to the public.

Your testing activities should include the following:

[3] http://www.firstresponder.gov/SitePages/SiteSearch/SiteSearch.aspx?k=WEA

- *Practice your established operating procedures that define the activities your office will take when planning and sending a WEA message, including:*
  - *exercising the process to decide to send a WEA message*
  - *exercising the WEA message approval process*
  - *exercising coordination activities with other organizations within your jurisdiction*
  - *exercising coordination activities with neighboring jurisdictions*
- *Practice accessing and using the software that you have chosen, including:*
  - *establishing the correct message parameters (severity, urgency, etc.)*
  - *defining the correct geographic area*
  - *crafting a readable message within the 90-character constraints, if using the CMAM text message generation option*

  Perform this practice while connected to the JITC Test Lab, not IPAWS-OPEN.
- *Verify your connections to IPAWS-OPEN. While it is not possible to fully verify your connection by sending a test message to IPAWS-OPEN, you can verify your ability to connect to the IPAWS-OPEN production server through the use of IPAWS-OPEN administrative messages. Your alert software can generate a getACK request (ping) and, if there are no communication or authentication errors, IPAWS-OPEN will respond with a reply (pong).*
- For further information, the reference to the entire report extracted above, please see http://www.firstresponder.gov/TechnologyDocuments/Wireless%20Emergency%20Alerts%20Best%20Practices.pdf

3.6 Expectations of Localized WEA testing by Commercial Mobile Service Providers

Commercial Mobile service Providers on the Testing Sub Group put forth the following basic expectations for a true end to end test from Alert Originator to the recipient of the alert:

- There would be no support required from the carriers in the activation of the test.
- All Localized WEA Test Messages must go through the FEMA IPAWS Federal Alert Gateway.
- In general, any single alert originator should issue a WEA test no more often than once a month.
- Localized WEA test messages should not be received by all subscribers. Test participants should “opt in” to receiving Localized WEA test messages. The default configuration should be “off” for reception of Localized WEA Test messages.
- Localized WEA Testing should use all CMSPs in the local alert area and not focus on a subset of CMSPs.
- CMSPs must have the option to reject a Localized WEA test request if the CMSP determines such testing would impact the CMSP network or ongoing operations.
- Localized WEA Testing impacts to devices should be standardized in the Joint ATIS-TIA Mobile Device Behavior Specification. Network impacts for supporting the test should be standardized in the appropriate Joint ATIS-TIA and 3GPP standards.
- Localized WEA tests will not be supported in legacy 2G or 3G or 4G devices.

Localized WEA testing will only be supported for new LTE devices capable of being configured for receiving the test messages.

- Recommend that any localized WEA tests message content be restricted to a length defined by the capabilities of the underlying technology and include the agency responsible for the test message and instructions to contact that agency (not the CMSP or 9-1-1) if there are any concerns:
    - "This is a WEA test initiated by Anytown Emergency Management. Please contact us with questions or concerns regarding this test"

3.6.1 Expectations of CMSP Support of Tests

Localized WEA Tests are designed to support local alert originators in developing and testing their procedures for issuing WEA alert messages; these tests should not be viewed as an exercise of CMSP infrastructure or mobile devices beyond normal WEA processing. Given that WEA is a voluntary service, CMSPs should not be obligated to provide support for these tests. With the number of alert originators signing up to initiate WEA messages, there potentially could be hundreds of Localized WEA Tests annually. The level of support required has the potential to overwhelm CMSP limited resources and detract from critical support for real alerts.

If major significant issues are encountered during a Localized WEA test (such as the test message not being transmitted), then it is recommended that the industry and government stakeholders (alert originators, FEMA, and CMSPs) develop a best practices ATIS/TIA standard for defining and reporting procedures for significant problems.

Alert originators should not have expectations that CMSPs will be able to provide support for debugging other issues such as geo-targeting of the test message, device configuration issues, determining why individual devices did not receive a message, delays in receipt of the message, etc. However, this does not preclude a CMSP and an alert originator from establishing a business relationship, including compensation, to provide contract support for a test.

3.7 Issues and Challenges with Testing Under Current Rules

3.7.1 Existing Testing Rules: Clarification or Waiver

The FCC's WEA rules only discuss required monthly testing (RMT) and gateway testing and do not provide guidance with regard to additional testing that may be undertaken. *See* 47 C.F.R. 10.350. As mentioned in the prior sections of this Report, participating commercial mobile service providers are obligated to participate in the RMT, which are scheduled for the third Wednesday of every month at 1 p.m. (ET). The RMTs consist of a WEA message delivery from the Federal Alert Gateway Administrator to the commercial mobile service

provider gateway within that provider's infrastructure. Pursuant to FCC rules,[4] a WEA required monthly test will be initiated only by the Federal Alert Gateway Administrator using a specifically designed test message that is defined by J-STD-101.[5] In addition to the RMT, Section 10.350 sets forth requirements for "Periodic C Interface Testing."[6] Participating commercial mobile service providers must participate in periodic testing of the interface between their gateway and the Federal Alert Gateway. In this instance, testing is not intended to assess the commercial mobile service provider's infrastructure as in the case of the RMT, but rather, its purpose is to ensure the availability and viability of both gateway functions. The use of real event codes or alert messages is not permitted for the periodic interface testing.[7]

The WEA rules require participating CMSPs to transmit test messages across their service area that optionally may be received by devices which are configured to receive the RMT. However, as referenced earlier in this Report, stakeholders now are evaluating the merits of end-to-end testing that would be involved the delivery of test messages to subscribers/test participants and would supplement the testing specifically referenced in the rules.

The FCC rules do not appear to prohibit such tests, or other forms of testing.[8]

3.7.2 Liability Protection and Implications of Additional Testing

Section 602(e) of the WARN Act provides very broad liability protection for the delivery, as well as the failure to deliver, wireless emergency alerts. Although the Section does not specifically address the extent of a commercial mobile service provider's exposure related to performing tests of the system, it contains broad language that appears to extend liability protection to such tests. Specifically, Section 602(e)(1)(A) states: "Any commercial mobile service provider . . . that transmits emergency alerts and meets its obligations under this title shall not be liable to any subscriber to, or user of, such person's service or equipment for – (A) ***any act*** . . . . related to the transmission of an emergency alert." It is reasonable to conclude that the broad scope of the liability protection provided by the phrase "any act . . . related to. . ." includes any testing associated with alert transmission via the system.

3.8 How WEA Message Content for Testing is Currently Derived

The Federal Alert Gateway is configured to automatically send the RMT message on the

[4] 47 C.F.R. 10.350(a)(4)
[5] *See* Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification (J-STD-101). Content of RMT is defined in J-STD-101 "This is a test of the Commercial Mobile Alert System. This is only a test."
[6] 47 C.F.R. 10.350(b).
[7] *Id.*
[8] *See* The Commercial Mobile Alert System, PS Docket No. 07-287, *Second Report and Order and Further Notice of Proposed Rulemaking*, 23 FCC Rcd 10765 (2008). "We will not require that CMS providers make available mobile device that support reception of the required monthly test. We do, however, allow CMS providers to choose to do so."

third Wednesday of each month at 1PM Eastern Time. The content of the RMT was defined in J-STD-101 as "This is a test of the Commercial Mobile Alert System. This is only a test."

The following chart is a swim lane diagram of the existing RMT process with descriptive text to describe the RMT process.

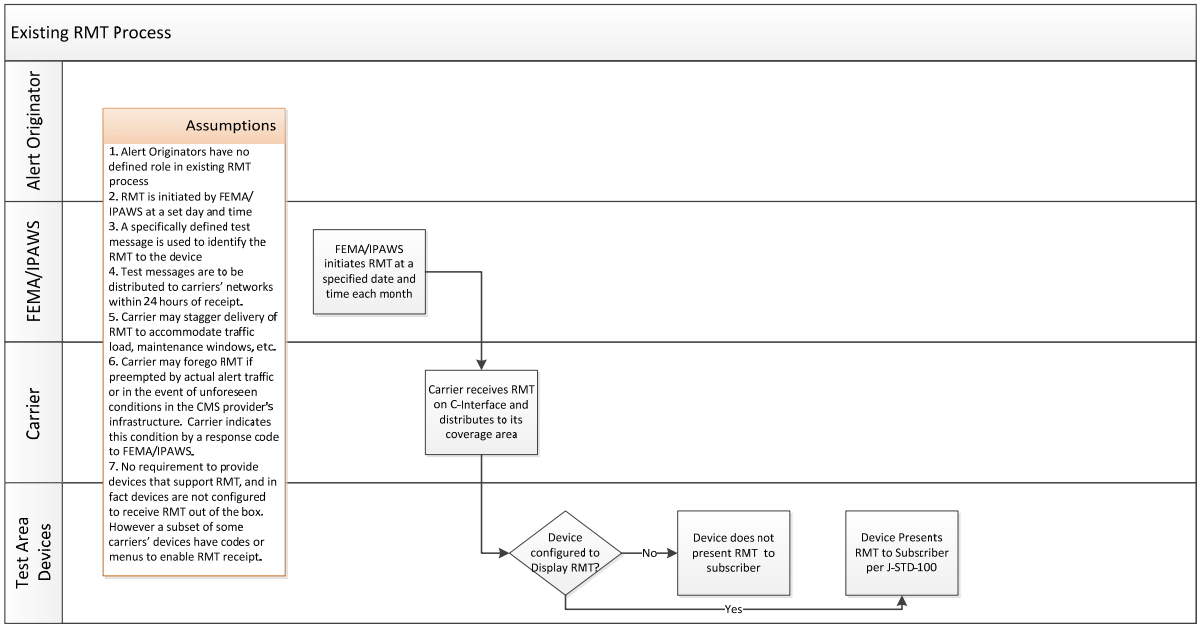


Figure 2 : Existing RMT Process

1. On the Third Wednesday of each month, FEMA/IPAWS issues a WEA Alert with the Message ID of "RMT". There is no geography with this alert, as the RMT is nationwide in scope, by standard.
2. Carriers receive the RMT and send it for broadcast to their radio elements configured for WEA.
3. As an option, certain devices may have been manufactured to receive the RMT upon the entry of a configuration code or through a menu on the device. Devices configured to receive the RMT will receive and display the RMT.

3.9 Backward Compatibility Issues

Current RMT as designed in standards identifies the RMT as a unique test message. WEA capable handsets receive the RMT, but do not present the RMT to the subscriber in any manner (audio, visual or vibration), unless the device is configured to receive the RMT. Implementation of RMT receipt on a device is a carrier or device OEM specific implementation option.

The RMT is processed similarly to a Presidential alert (which notifies all cells in a carrier footprint). There is no geography selection associated with the RMT in current standards; RMTs are assumed to be nationwide and occur once per month.

3.10 Impact to Standards

Cell broadcast and Public Warning System standards are international in scope, and any

modification to existing designed RMT logic and process will likely require a change to both 3GPP standards as well as the standards from ATIS and TIA that enable WEA in the United States. Therefore any changes to RMT must take into account worldwide standards and remain cognizant of worldwide handsets, requirements, etc.

As stated above, existing standards contemplate a message ID that emulates the presidential message. The User device, unless specifically configured to receive the RMT, ignores this message. Any addition or change to existing testing procedures would need a review of the effects of the solutions upon the following standards/documents and SDOs.

- A/B Interface between Alert Originator and FEMA/IPAWS allow for LWT and Operational Considerations
- ATIS/TIA Specification Updates
  - ATIS/TIA J-STD-100 (Handset Standard)
  - ATIS/TIA J-STD-101 (C-Interface Specification)
  - ATIS/TIA J-STD-102 (C-Interface Test Specification)
- ATIS Specification Updates
  - ATIS-0700010 (CMAS via EPS)
  - ATIS 0700006 (CMAS via GSM/UMTS)
- 3GPP & OASIS
  - Depending upon the technical solution developed 3GPP and OASIS CAP standards might need to be modified.
  - The IPAWS CAP profile for WEA may need to be modified.

3.11 Issues and Concerns with WEA End-to-End Testing

Concerns have been expressed by wireless carriers that transmitting live WEA test messages, which sound and look like actual WEA messages, to all users in a geographic area could negatively impact the WEA service.

For example, in December 2013, a WEA message that sounded on cellphones in Southern California was determined to have been a test message using live alert codes. The alert read "THIS IS ONLY A TEST," and generated news stories related to this incorrectly sent test, how it had interrupted the public.[9] As there was apparently little or no outreach prior to the test, this event demonstrates how these types of tests might confuse the general public.

Whereas radio, TV, outdoor warning siren and EAS testing are performed routinely, these

[9] See http://www.latimes.com/local/lanow/la-me-ln-emergency-alert-test-from-monterey-park-causes-confusion-anger-20131204,0,6187721.story and http://ktla.com/2013/12/04/emergency-alert-sounds-on-phones-across-socal/ for news stories related to this incident See http://www.latimes.com/local/lanow/la-me-ln-emergency-alert-test-from-monterey-park-causes-confusion-anger-20131204,0,6187721.story and http://ktla.com/2013/12/04/emergency-alert-sounds-on-phones-across-socal/ for news stories related to this incident

tests are not as intrusive to citizens' everyday lives as a cell phone going off. The majority of citizens carry cell phones while going about their everyday life – including in schools, doctor's offices, business meetings, etc. Live testing to every citizen has the potential to disrupt their activity to the point they turn off WEA, complain to the carrier's customer care, call 9-1-1, or other actions. Even with extensive education, live testing still raises concerns that subscribers would opt out of WEA entirely due to alert fatigue.

4 Subgroup Recommendations

4.1 Recommendations for Localized WEA Testing

The subgroup pursued an approach to WEA testing which best meets alert originator objectives (i.e., system verification, operator proficiency, and public awareness) and requirements while minimizing overall risk. The options considered by the subgroup are listed in Appendix E.

Of the three options, the WG-2 Subgroup concluded and therefore recommends that Option 2 (Alerting Authorities Conduct WEA Test to Opt-in Participants) achieves the maximum objectives possible for an acceptable level of risk. Thus, alert originators should be authorized to conduct WEA testing in this manner.

The WG-2 Testing Subgroup recommends the FCC amend Part 10 rules to allow for a Localized WEA Testing procedure which is an opt-in test, with the default configuration of being Opt-Out. The Testing Subgroup also recommends that the relevant industry standards bodies modify all appropriate standards to define a common standardized method for supporting the Opt-in test.

Whether a test to the public, or to an Opt-in group, Alert Originators should always include language that the message being sent is clearly a test message and which agency is responsible for initiating the test. It should also include all the currently required elements of a live message such as the source of the warning message, set the levels of urgency, severity and certainty and the following as space allows;

- Specific Hazard: What is/are the hazards that are threatening? What are the potential risks for the community?
- Location: Where will the impacts occur? Is the location described so those without local knowledge can understand their risk?
- Timeframes: When will it arrive at various locations? How long will the impacts last?
- Protective Behavior: What protective actions should people take and when? If evacuation is called for, where should people go and what should they take with them?

Note the test message will have the message length constraints based upon the CMSP technology used to deliver the test and follow the procedures that are developed in an ATIS/TIA standard.

4.2 Recommendation for Waivers

The WG-2 Testing Subgroup recommends that the FCC clarify that WEA end-to-end testing beyond the RMT is not precluded by any of its existing rules. To the extent the FCC finds that its current rules preclude such testing, the FCC should identify those rule provisions that would be implicated and waive those requirements.[10] Alternatively, the Commission could initiate a proceeding to modify the conflicting requirements in accordance with the "Opt-in" WEA Testing paradigm described herein.[11] Given the importance of WEA and testing, the Testing Subgroup recommends that an interim waiver of the rules be granted to permit end-to-end testing pending the conclusion of any rulemaking, standardization and development activities.

4.3 Recommendation for Liability Protection

Because there is no specific mention of WEA testing in the WARN Act's liability protection provision, there may be some question of whether such protections are afforded to other key efforts affiliated with the transmission of wireless emergency alerting via WEA. To this end, the WG-2 Testing Subgroup recommends that the FCC confirm that Section 602(e) of the WARN Act covers testing. In particular, the FCC should work with Congress or through other legislative means to clarify that the Section 602(e) protections against liability afforded to commercial mobile service providers extend to any WEA testing as this is a vital/essential function associated with alert transmission.

4.4 Recommendation on Reporting Procedures

No formal procedures exist for the reporting of WEA-related problems among alert originators, FEMA, and CMSPs. Per the discussion in Section 3.6.1, it is recommended that industry and government stakeholders (alert originators, FEMA, and CMSPs) develop a best practices ATIS/TIA standard for defining and reporting on significant problems. These procedures would be used to report significant issues encountered during WEA testing.

[10] *See e.g.*, The Commercial Mobile Alert System, PS Docket No. 07-287, *Order*, 28 FCC Rcd 1460 (Rel. Feb. 25, 2013). "Thus, to the extent the broadcast of the WEA Attention Signal during the PSAs could be construed as being subject to the Section 11.45 general prohibition on the transmission of the EAS Attention Signal other than during specified emergencies or lawfully authorized tests, or to the extent Section 10.520 can be read as including a similar prohibition regarding WEA Attention Signals, we hereby waive those rules, subject to the conditions and limitations discussed herein."

[11] See Section 3.11.3 of this document

Appendix A: Referenced Documents

http://www.dailykos.com/story/2012/03/09/1072713/-What-are-these-RMT-Alerts#
http://ktla.com/2013/12/04/emergency-alert-sounds-on-phones-across-socal/
http://www.latimes.com/local/lanow/la-me-ln-emergency-alert-test-from-monterey-park-causes-confusion-anger-20131204,0,6187721.story

Appendix B: Acronyms

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

Acronym	Definition
3GPP	3rd Generation Partner Project
3GPP2	3rd Generation Partnership Project 2
AO	Alert Originator
ATIS	Alliance for Telecommunications Industry Solutions
CMAS	Commercial Mobile Alert System
CMSAAC	Commercial Mobile Service Alert Advisory Committee (of the FCC)
CMSP	Commercial Mobile Service Provider
EOC	Emergency Operations Center
FCC	Federal Communications Commission
LWT	Localized WEA Testing
RMT	Required Monthly Test
SDO	Standards Development Organization
WEA	Wireless Emergency Alerts

Appendix C: Glossary

This appendix contains the glossary associated with this report.

Term	Definition
3GPP	The 3rd Generation Partnership Project (3GPP) is a collaboration agreement that was established in December 1998. The collaboration agreement brings together a number of telecommunications standards bodies which are known as "Organizational Partners".
Access Provider	An access provider is any organization that arranges for an individual or an organization to have access to the Internet.
Alliance for Telecommunications Industry Solutions (ATIS)	A U.S.-based organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. http://www.atis.org/
Broad Scope LWT	LWT test is which received by all devices in an alert area without any additional configuration required in the device to have the device
FCC Part 10 Rules on WEA	Enabling FCC rules related to the WEA service, to include current WEA testing rules.
Geo Location	Latitude, longitude, elevation, and the datum which identifies the coordinate system used.
Geocoding	Translation of one form of location into another, typically a civic address into an x, y coordinate.
Limited Scope LWT	LWT test which is received by all devices in an alert area which is processed as a Silent WEA Test.
Live WEA Test	A WEA message sent using actual WEA codes and is received by all WEA capable devices, which is intended in its use to test the system. The only notification that this is a test is the content of the message itself.
Localized WEA Testing	Concept of testing WEA at the city, county, parish, borough, state or regional level, using a polygon or FIPS code to test WEA, rather than the existing Required Monthly Test which is nationwide in scope.
Silent WEA Test	A WEA message sent using a WEA message ID that is recognized by a WEA capable device as a localized WEA test message. Notifications are only provided by devices which are configured to accept the test ID associated with localized WEA test messages or are otherwise configured to receive the test. The test alert is "silent" to users with devices not configured to receive the test.
Working Group (WG)	A group of people formed to discuss and develop a response to a particular issue. The response may result in a Standard, an Information Document, Technical Requirements Document or Liaison.

Appendix D: Testing Outreach Example

The following document is an example of an educational outreach effort related to WEA, courtesy of Johnson County Emergency Management & Communications, Olathe, Kansas

Wireless Emergency Alerts

In weather emergencies, warnings can save lives. But traditional warning methods such as television, radio and outdoor sirens don't always reach everyone.

Emergency officials now have a new way to send warnings directly to cell phones in affected areas — Wireless Emergency Alerts (WEAs).

These short messages — less than 90 characters — may look like a text message, but unlike texts, which are sent directly to your phone number, these warnings are broadcast to all phones within range of designated cell towers.

The alerts will tell you the type of threat or warning, the time it goes into effect, when it was issued, the issuing agency and the time it will expire. You'll need to turn to other sources, such as television or your NOAA All-Hazards radio, to get more detailed information about what is happening and what actions you should take.

For illustration only. Actual message appearance will vary.

Key Things to Know:

- WEA messages may look like a text, or appear over your home screen.
- The alert message will include a unique ringtone and vibration.
- You will never be charged for WEA messages.
- Emergency alerts will not interrupt any calls or downloads in progress. If you're on the phone when the alert goes out, you'll get the message when you end your call.
- You need not have GPS or any other special features turned on to receive the alerts.
- The system does not identify your location or phone number — it simply sends the message to all devices in a given area.
- If you're on the road and enter an area with an active warning, you'll receive a WEA message as soon as you come within range of one of the affected cell towers.

Is your phone ready for WEA?

If you have an older model phone, you may not receive the Wireless Emergency Alerts. This feature is built in on newer cell phones. Check with your service provider to find out if your phone is WEA-capable.

MEMC
Metropolitan Emergency Managers Committee

PrepareMetroKC.org
Make a supply kit. Have a plan. Stay informed.

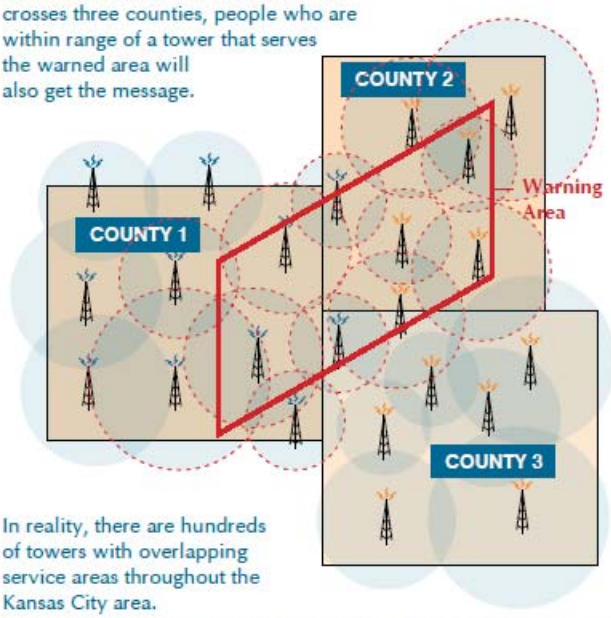
Cell tower geography may lead to some overwarning

Because cell towers broadcast in a radius, or circle, their coverage areas don't line up neatly with county boundaries or warning polygons. This means you may receive warnings if you're on the outskirts of the warned area.

The alerts are delivered directly from cell tower to cell phone through a one-way broadcast. The system does not track or locate individual cell phones or phone numbers — it simply broadcasts to all phones within range. Unfortunately, in some cases, this may result in overwarning.

For example, when a tornado warning is issued for a particular area, it will go to all towers that serve that area. Towers in urban areas generally serve a radius of two to five miles, and in rural areas up to 10 miles, so the warning message may reach a little beyond the actual warning boundaries.

As this simplified illustration shows, when a warning is issued for a polygon that crosses three counties, people who are within range of a tower that serves the warned area will also get the message.



In reality, there are hundreds of towers with overlapping service areas throughout the Kansas City area.

Wireless Emergency Alerts: Three Types of Warnings

The Wireless Emergency Alert System can be used to broadcast three types of emergency alerts:

- **PRESIDENTIAL ALERTS** — Issued by the U.S. President in the event of a nationwide emergency.
- **IMMINENT THREAT ALERTS** — Typically issued by the National Weather Service; in the Kansas City metropolitan area, these could include both "extreme" warnings (tornado and high winds) and "severe" warnings (flash floods).
- **AMBER ALERTS** — Issued by law enforcement to share information about a child abduction.

No president has ever yet had to issue a presidential alert, but should one become necessary, cell phone providers are required to broadcast it to all WEA-capable phones.

Cell phone users may choose to opt out of imminent threat and/or AMBER alerts, but the procedures vary by carrier. Some providers will allow customers to opt out of one or the other — or opt out of severe warnings but still get extreme alerts — while others only allow you to opt out of both. Contact your wireless provider for more information.

The Metropolitan Emergency Managers Committee strongly encourages all residents not to opt out of these potentially life-saving messages.

To learn more, contact your local emergency management office or wireless service provider. Visit www.preparemetrokc.org for more information on emergency preparedness.

Appendix E: WEA Testing Options

The Testing sub working group discussed a number of options related to how to implement the testing requested by the Alert Originators. The tables in this appendix are a summary of the discussion points surrounding the various options.

Option 1: Allow Alert Originators to Utilize the Current RMT Process

Currently, FEMA conducts a nationwide Required Monthly Test (RMT) which is delivered to handsets but is not displayed on WEA capable devices by default and can only be monitored on some WEA-capable devices if enabled. The RMT may not be delivered immediately and may be held up to 24 hours. This option extends a similar RMT capability to authorized WEA alerting authorities, with an option of adding geotargeting to the RMT.

This option bears very little similarity to an actual WEA activation; RMTs are designed to exercise the FEMA to CMSP interface and CMSP infrastructure. There is very low risk, but little if any benefit in the areas of system verification, alert originator proficiency and public awareness. Alert originators expressed concern that this approach yields no knowledge about the actual WEA broadcast coverage (i.e., under-reach/overreach) in their area of responsibility which otherwise might weigh in on future decisions to activate WEA, WEA message content, and/or information which must be conveyed over other communication channels in order to maximize message clarity and minimize public confusion.

The following table shows the risks associated with this option as well as how those risks could be mitigated.

Risk	Mitigation
FEMA RMTs have resulted in little or no impacts to alert originators, wireless operators or FEMA IPAWS. Extending the capability to alert originators would do little to increase risk.	None

The following table describes the extent to which this option meets the needs identified by alert originators in the FEMA poll.

System Verification	Alert Originator Proficiency	Public Awareness
Little new is being done except that any alerting authority may issue what essentially amounts to a silent test. Thus, little can be learned. Carriers may queue or stage the alert for later	Provides little if any contribution to alert author proficiency. Alert authors essentially operate in a risk free training mode. There is no real-life feedback regarding human or system related delays, failures, inaccuracies, errors, or other	Does not expose the general public to an actual WEA. Particularly in areas which rarely receive WEA messages, the public may not readily respond to a real WEA message, the mobile device user may not know if WEA is enabled on their device, and

dissemination up to 24 hours later. Delayed delivery makes coordinated testing (with sirens for instance) impossible. Any technical problems (i.e., alerting tools, communication lines, wireless networks, devices, etc.) most likely go unnoticed and unresolved.	issues which may otherwise cause public confusion in a real WEA activation. Overall, there are minimal lessons learned and little operational experience is gained by the alert author.	may not know if WEA-related software/hardware functions correctly.

Option #2 – Alerting Authorities Conduct WEA Test to Opt-in Participants

A WEA alerting authority may conduct a scheduled Local WEA Test (LWT) which targets cooperating partners (e.g., Community Emergency Response Teams, amateur radio operators, Skywarn spotters, civic groups, First Responders, etc.) and other interested parties who may provide feedback to the alert originator. Participants must opt-in in order to monitor the test.

This option bears similarity to an actual WEA activation. There are significant benefits in the areas of system verification, alert originator proficiency, and public awareness. Alert originators will educate participants prior to testing. The wireless industry advises that this option requires standards change and development work for devices, CMSP infrastructure, and the FEMA IPAWS Federal Alert Gateway.

The end-to-end process flow for this testing is shown in figure 3 and described below.

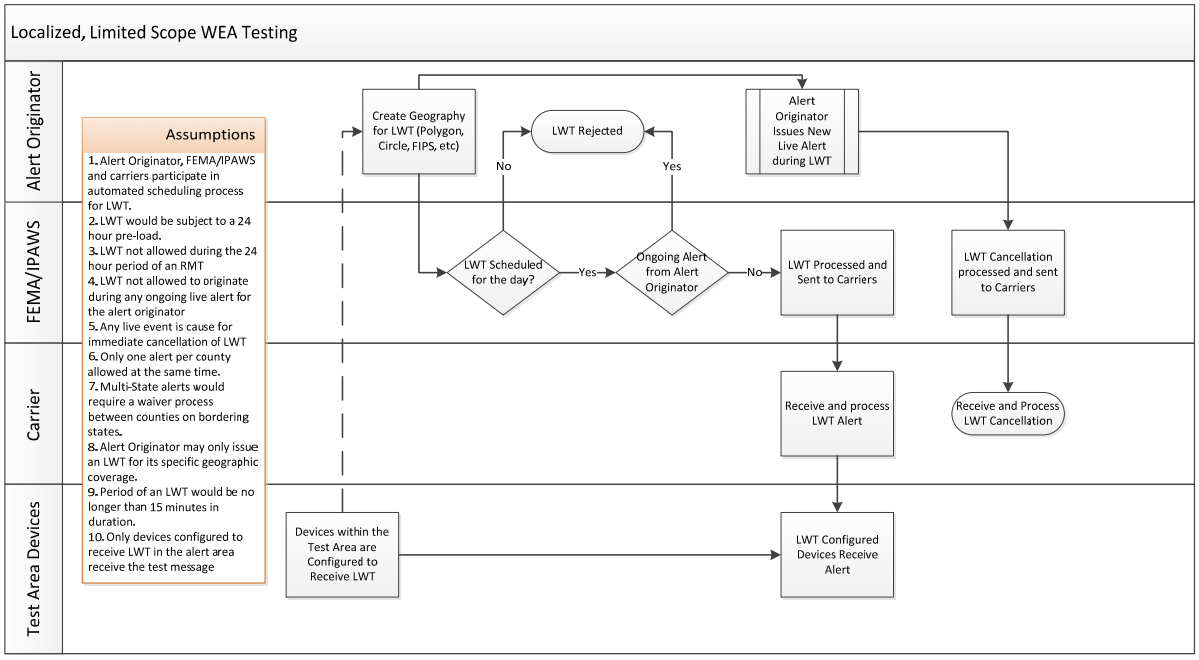


Figure 3: Process for alerting authorities to conduct WEA testing with opt-in participants

1. Prior to the LWT, the Alert Originator (AO) coordinates with their testing participants on the configuration of their device to receive the LWT.
2. The AO creates a specific geography for the content of the test, crafts the content of the test message and submits to FEMA IPAWS.
3. FEMA/IPAWS checks it systems to determine if the LWT was scheduled with them for that particular day and that there is not an ongoing live alert from within or near the particular LWT alert area.
4. FEMA/IPAWS sends the LWT to carriers which have coverage within the alert area.
5. Carriers then receive and process the LWT
    a. If during the processing of the LWT a live alert is received for the LWT alert area, FEMA/IPAWS shall initiate an immediate cancellation to the carriers for

the LWT and initiate the live alert.

b. Carriers will cancel the LWT and begin processing the live alert.

6. Test participants and others who have configured their devices configured for LWT then receive the LWT.

The assumption of this testing process is that it would be an alert not seen or heard by the general population, but only received by persons who had specifically opted in on their device to receive the test, such as volunteers and interested parties who partner with the Alert Originators on a routine basis. The subscriber would also have the ability to Opt-out of receiving the LWT on their device.

The following table shows the risks associated with this option as well as how those risks could be mitigated.

Risk	Mitigation
Small risk of wireless operator and emergency call centers receiving from inquiries from the general public regarding problems or confusion associated with the test.	Test participants, news, and electronic media will be educated prior to the test, so that exposure of the issues is limited to a savvy group who best understands the nature and purpose of the testing (i.e., looking for lessons learned, familiarize people with the service, and to enhance readiness for a real-life event).

The table below describes the extent to which this option meets the needs identified by alert originators in the FEMA poll.

System Verification	Alert Originator Proficiency	Public Awareness
Provides end to end verification. Since a sampling of the population is monitoring the test, some problems with the system (i.e., alerting tools, communication lines, wireless networks, devices, etc.) could be detected and some could go undetected.	Is a realistic environment for alert author proficiency. Alert authors operate in an operational mode. Testing will provide some real-life feedback regarding human or system related delays, failures, inaccuracies, errors, or other issues which may otherwise cause public confusion in a real WEA activation. Lessons will be learned, but savvy test recipients may not be an accurate sample of the general public at large. Thus, feedback is somewhat representative of the general	Test provides limited public exposure to an actual WEA. However, members of the news and electronic media could be organized to participate in the test, report on it, and provide tips to the general public which enhance overall public awareness.

	public.	

Option #3 – Alerting Authorities Conduct WEA Test to Opt-out Participants

A WEA alerting authority may conduct a scheduled Local WEA Test (LWT) which targets their entire population. These tests are opt-out.

This option is nearly identical to the factors at play during an actual WEA activation. There are high levels of benefit in the areas of system verification, alert originator proficiency, and public awareness. Wireless industry expresses great concern that wireless operator and emergency call centers will be inundated with customer inquiries and insists that test messages clearly direct recipients to the agency initiating the test for more information. Alert originators must ensure extensive public education has been performed prior to testing in order to minimize impacts on wireless operator and emergency call centers. Wireless industry advises that this option will take several years to implement in order to get new devices to the general public which support this type of testing. Moderate requirements and standards work would be necessary as well.

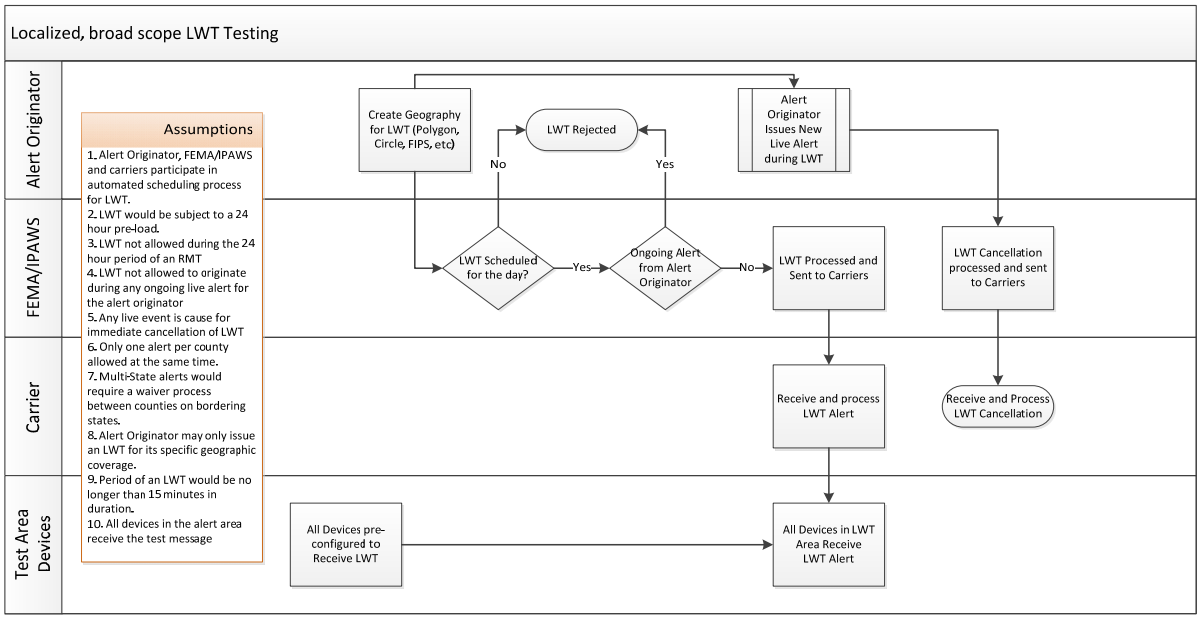


Figure 4: Broad Scope LWT testing

1. It is assumed that for Broad Scope LWT, all devices have been pre-configured to receive the LWT. There may be an opt-out for the LWT
2. The AO creates a specific geography for the content of the test, crafts the content of the test message and submits to FEMA IPAWS.
3. FEMA/IPAWS checks it systems to determine if the LWT was scheduled with them for that particular day and that there is not an ongoing live alert from within or near the particular LWT alert area.
4. FEMA/IPAWS sends the LWT to carriers which have coverage within the alert area.
5. Carriers then receive and process the LWT
    a. If during the processing of the LWT a live alert is received for the LWT alert area, FEMA/IPAWS shall initiate an immediate cancellation to the carriers for the LWT and initiate the live alert.
    b. Carriers will cancel the LWT and begin processing the live alert.

6. All devices configured for LWT whose users have not opted out of LWT receive the LWT.

The following table shows the risks associated with this option as well as how those risks could be mitigated.

Risk	Mitigation
Embarrassing failures or problems may be exposed to the general public which may result in people turning off WEA and/or reduction in public support for the service.	Extensive education of the general public, news, and electronic media can be conducted prior to the test, so that people understands the nature and purpose of the testing (i.e., looking for lessons learned, familiarize people with the service, and to enhance readiness for a real-life event).
Wireless operator and emergency call centers may be stressed by inquiries from the general public and news media regarding problems or confusion associated with the test. For example, in California a test message was accidentally sent as a production WEA message which resulted in large number of complaints and turning off of WEA on mobile devices. The same is true for Amber Alerts which is also causing people to turn off WEA.	

The following table describes the extent to which this option meets the needs identified by alert originators in the FEMA poll.

System Verification	Alert Originator Proficiency	Public Awareness
Provides end-to-end verification. Since the general population is exposed to the test, any problems with the system (i.e., alerting tools, communication lines, wireless networks, devices, etc.) are likely to be detected.	Is a realistic environment for alert author proficiency. Alert authors operate in an operational mode. There is real-life feedback regarding human or system related delays, failures, inaccuracies, errors, or other issues which may otherwise cause public confusion in a real WEA activation. Feedback and lessons learned are representative of the general public.	There is maximum public awareness of WEA.

Appendix F: Existing WEA Standards

Number	Title	Description
ATIS-0700006	CMAS via GSM/UMTS Cell Broadcast Service Specification	This ATIS specification defines the requirements, architecture, interfaces, call flows, and message formatting for the support of CMAS on the GSM Cell Broadcast Service.
ATIS-0700006.a	Supplement A to ATIS-0700006, CMAS via GSM/UMTS Cell Broadcast Service Specification	This supplement provides errata and clarifications to the published version of ATIS-0700006, CMAS via GSM/UMTS Cell Broadcast Service Specification.
ATIS-0700007	Implementation Guidelines and Best Practices for GSM/UMTS Cell Broadcast Service	This ATIS specification provides implementation guidelines and best practices for the implementation of CMAS on the GSM Cell Broadcast Service. Detailed call flows regarding the behavior of CMAS on the air interface is included in this specification.
ATIS-0700008	Cell Broadcast Entity (CBE) to Cell Broadcast Center (CBC) Interface Specification	This ATIS specification defines an interface and message format for Cell Broadcast messages from the Cell Broadcast Entity (CBE) to the Cell Broadcast Center (CBC). The 3GPP specifications do not define this interface. The CBE is the entity which creates the Cell Broadcast messages for broadcast by the CBC. In CMAS, the CMSP Alert Gateway is the CBE.
ATIS-0700010	CMAS via EPS Public Warning System Specification	This ATIS specification defines who CMAS is supported in the LTE environment since Cell Broadcast does not exist in the LTE environment. This ATIS specification defines the requirements, architecture, interfaces, call flows, and message formatting for the support of CMAS on LTE.
ATIS-0700010.a	Supplement A to ATIS-0700010, CMAS via EPS Public Warning System Specification	This supplement provides errata and clarifications to the published version of ATIS-0700010, CMAS via EPS Public Warning System Specification.
ATIS-0700012	Implementation Guidelines for CMAS Supplemental Information Retrieval	This ATIS specification defines how the CMAS Alert Gateway could retrieve CMAS Supplemental Information from the Federal Alert Gateway. The primary supplemental information is the alert message in Spanish. As of November 2013, FEMA has not agreed to implement this specification.
ATIS-0700013	Implementation Guidelines for Mobile Device Support of Multi-Language CMAS	This ATIS specification defines the guidelines for mobile devices which support CMAS in multiple languages (e.g., English & Spanish). This specification applies to GSM, UMTS, and LTE. This specification is also applicable in the international environment. This specification will be applicable whenever CMAS in Spanish is implemented.

Number	Title	Description
ATIS-0700014	Implementation Guidelines for CMAS Handling of CMAS Supplemental Information Broadcast	This ATIS specification describes the functionality of Cell Broadcast based CMAS when the CMAS messages are being broadcast in both two languages (e.g., English and Spanish). This specification will be applicable whenever CMAS in Spanish is implemented.
J-STD-100	Joint ATIS/TIA CMAS Mobile Device Behavior Specification	This Joint ATIS/TIA specification defines the behavior of the mobile device when it receives a CMAS message.
J-STD-100.a	Supplement A to J-STD-100, Joint ATIS/TIA CMAS Mobile Device Behavior Specification	This supplement provides errata and clarifications to the published version of J-STD-100, Joint ATIS/TIA CMAS Mobile Device Behavior Specification. This specification applies to both 3G and 4G.
J-STD-101	Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification	This Joint ATIS/TIA specification defines the interface between the Federal Alert Gateway and the CMSP Alert Gateway. This interface is commonly called the "C Interface" because of its location on the architecture diagram (see Figure 1).
J-STD-101.a	Supplement A of J-STD-101, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification	The FCC 2nd Report and Order on CMAS defines an optional method for the distribution of CMAS messages from the Federal Alert Gateway to the CMSP Alert Gateway via the Public Television broadcast network. This supplement defines the C Interface Over The Air (C-OTA) from the Public Television Digital Television (DTV) Receiver and Decoder to the CMSP Gateway. There are no known implementations of this capability.
J-STD-101.b	Supplement B of J-STD-101, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification	This supplement provides errata and clarifications to the published version of J-STD-101, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification.
J-STD-102	Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Test Specification	This Joint ATIS/TIA specification defines the test environment and test cases to test the interface between the Federal Alert Gateway and the CMSP Alert Gateway. This interface is commonly called the "C Interface" because of its location on the architecture diagram.
J-STD-102.a	Supplement A of J-STD-102, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Test Specification	This supplement provides errata and clarifications to the published version of J-STD-102, Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Test Specification.
TIA-1149	Commercial Mobile Alert Service (CMAS) over CDMA Systems	This standard provides a specification for CMAS over CDMA Systems.

Number	Title	Description
TIA/EIA/IS-824	Generic Broadcast Teleservice Transport Capability - Network Perspective	This Telecommunications Industry Association (TIA) standard provides a specification for the broadcast capability used in CDMA systems.
3GPP2 S.R0030-A	Broadcast/Multicast Services – Stage 1 Revision A	This document defines the functional characteristics and requirements of Broadcast/Multicast Services.
3GPP2 C.S0077-0	Broadcast Multicast Service for CDMA2000 1x Systems	This document defines requirements for support of the Broadcast/Multicast Service (BCMCS) capability on cdma2000® 1x spread spectrum systems.
3GPP2 X.S0022-A	Broadcast and Multicast Service for cdma2000 Wireless IP Network	This document defines core network protocols and procedures for support of the Broadcast-Multicast Service (BCMCS) for cdma2000® networks.
3GPP TS 23.041	3GPP Technical realization of Cell Broadcast Service (CBS)	This 3GPP specification for Cell Broadcast service includes the global requirements for the Commercial Mobile Alert Service (CMAS) and the Japanese Earthquake and Tsunami Warning System (ETWS).
3GPP TS 25.419	UTRAN Iu-BC Interface: Service Area Broadcast Protocol (SABP)	This 3GPP document specifies the *Service Area Broadcast Protocol (SABP)* between the Cell Broadcast Centre (CBC) and the Radio Network Controller (RNC).
3GPP TS 23.038	Alphabets and language-specific information	This 3GPP document defines the character sets, languages and message handling requirements for SMS, CBS and USSD.
3GPP TS 23.401	General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access	This 3GPP specification defines the Stage 2 architectural service description for the Evolved 3GPP Packet Switched Domain - also known as the Evolved Packet System (EPS). The Evolved 3GPP Packet Switched Domain provides IP connectivity using the Evolved Universal Terrestrial Radio Access Network (E-UTRAN). The specification covers both roaming and non-roaming scenarios.
3GPP TS 25.324	RAN Broadcast/Multicast Control (BMC)	This 3GPP document provides the description of the Broadcast/Multicast Control Protocol (BMC). This protocol adapts broadcast and multicast services on the radio interface.
3GPP TR 25.925	Radio Interface for Broadcast/Multicast Services	This 3GPP document provides a general overview on radio interface related aspects of broadcast/multicast services. This report covers stage 2 and stage 3 aspects of the radio interface.
3GPP TS 29.168	Cell Broadcast Centre interfaces with the Evolved Packet Core; Stage 3	This 3GPP document describes the procedures and protocols used on the interface between the Mobility Management Entity (MME) and the Cell Broadcast Center (CBC).

Number	Title	Description
3GPP TS 36.331	Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification	This 3GPP document specifies the Radio Resource Control protocol for the UE-E-UTRAN radio interface.
3GPP TS 44.012	Short Message Service Cell Broadcast (SMSCB) support on the mobile radio interface	This document provides radio support for SMSCB, a service in which short messages may be broadcast from a PLMN to Mobile Stations (MS)s.
OASIS Standard CAP V1.2 (2010)	Common Alerting Protocol[12]	This document provides an open, non-proprietary digital message format for all types of alerts and notifications.

[12] This document is available from the Organization for the Advancement of Structured Information Standards (OASIS) https://www.oasis-open.org/standards