Archived Content

Wireless Emergency Alerts

System Enhancement Recommendations

July 2013

Homeland Security

Science and Technology

WIRELESS EMERGENCY ALERTS

SYSTEM ENHANCEMENT RECOMMENDATIONS

Homeland Security

Science and Technology

July 2013

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

EXECUTIVE SUMMARY

This document describes several recommended enhancements for the operation, performance, and maintenance of the Wireless Emergency Alerts (WEA), formerly known as the Commercial Mobile Alert Service (CMAS). The recommendations are partially based on the results of a previous Computer Model and Simulation Results study undertaken as part of the WEA Program at The Johns Hopkins University Applied Physics Laboratory for the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T). In addition to this study, potential use cases of WEA and engineering best practices for secure and highly reliable systems were considered for inclusion in this document.

The following system enhancements are recommended for the WEA system. The rationale for each of these recommendations is described in the main body of this document, along with an overview of the recommended solutions and potential benefits. Implementation details of the recommended solutions are not described in depth in this document, but are deferred for future consideration.

The recommendations presented involve a number of important technical, programmatic, and policy decisions that must be made or endorsed by the Federal Communications Commission (FCC), Federal Emergency Management Agency (FEMA), DHS, Commercial Mobile Service Providers (CMSP), the Alert Originator (AO) community, and state and local first responders. The success of the WEA service strongly depends on its adoption by the alert origination community and the public. The evolution of the WEA system must be coordinated to answer the needs of its users.

- Introduce Multi-Level Priority – WEA currently assigns message prioritization equally among alerts and processes messages in a First In First Out order, with the exception of Presidential alerts. Implementation of additional priority levels would allow WEA to process time-critical alerts (e.g., earthquake and tornado warnings) before other less-time-critical alerts (e.g., tropical storm warnings). This would reduce the end-to-end latency experienced by time-critical alerts when a WEA network element experiences congestion due to an excessive number of messages or commercial cell broadcast traffic.

- Implement Management Plane Services and Protocols – Currently there is no end-to-end WEA system management capability. System management for each WEA component operates independently from other components. Defining and implementing a common WEA management plane would allow for new end-to-end system management services, such as enabling AOs to monitor system status and notifying AOs when alerts are successfully broadcast. This would enhance the experience of AOs using WEA, as it would better enable them to assess system performance, plan their usage of the system, and better use existing capabilities of the cellular infrastructure.

- Use Optimized WEA Broadcast Repetition Intervals – CMSPs that provide WEA service retransmit WEA messages several times to maximize the number of citizens that receive the alert. There is a tradeoff between alert reception latency and the amount of cellular network and handset resources (e.g., transmission bandwidth and handset battery power) consumed by repeated broadcasts. Choosing a small repetition interval for retransmissions reduces alert reception latency, but uses more transmission bandwidth and handset battery power. Therefore, optimizing the intervals for alert retransmissions would ensure

that the greatest number of cellular devices will receive alert messages in the shortest amount of time, minimizing cellular network and handset resource usage.

- Increase Infrastructure Resilience – Resilience of the WEA infrastructure against failures of system components (such as network connections and data centers) can be increased by supporting backup communication channels or backup data centers. This would incur additional cost, but increase system availability during and after major disasters.

- Implement Mutual Trustworthy Platform Verifications – Various WEA system components may contain malicious software, which can be used by an adversary to issue false public alerts and warnings. Implementing Mutual Trustworthy Platform Verifications would verify the integrity of software running on WEA computer platforms. This would ensure that systems are in a trustworthy state and comply with the information assurance guidelines for WEA operation.

- Enhance the Accuracy of Geo-Targeting – The geo-targeting precision of WEA can be improved beyond the cell site or cell sector granularity that is possible today. The recommended improvement is based on broadcasting alerts to an area wider than the affected area and making use of the location awareness of mobile devices, so that a user is notified of an alert only if the mobile device is inside the affected area. These enhancements would prevent missed alerts caused by geo-targeting inaccuracy and reduce over alerting the public with irrelevant messages. This is expected to encourage more widespread adoption of WEA by emergency managers and the public.

- Utilize Geographical Emergency Affinity Subscriptions – Currently, a WEA message can only be received in and around the affected area related to that message. The recommended enhancement would allow the public to be notified when a WEA message is issued to their home area, even if they are physically outside that area at the time the alert message is broadcast.

- Implement Post-Disaster WEA Mode – Major disasters will potentially damage cellular networks and impact the ability to disseminate post-disaster WEA messages. For example, major hurricanes and earthquakes can cause random physical destruction to cellular radio transmission equipment (cell site antennas or complete cell towers). This would cause WEA coverage gaps for the affected CMSPs. The recommended enhancement is based on cooperation among CMSPs after disasters to allow subscribers of one CMSP to receive WEA messages from other CMSPs. This would allow continuity of WEA service during and after a disaster. The recommended enhancement would also facilitate emergency communications with the public via cellular devices using a temporary cellular infrastructure that can be deployed by first responders.

- Increase Text Message Length – Currently, WEA messages are limited to 90 characters because of a requirement to transmit the message using only a single "page" of cell broadcast. On the other hand, cell broadcast supports multiple page messages. The recommended enhancement is to modify the requirement so that WEA can use multiple pages of cell broadcast. This would allow the transmission of longer messages, which can convey more information to the public.

- Enhance Multimedia Support – WEA service currently supports only text messages. It is recommended that WEA also supports audio and video content in alerts. This would convey more information to the public about the situation and the required action.

The DHS S&T WEA Program Management Office should work with the National Telecommunications and Information Administration and the FCC to establish a technically focused Advisory Group to guide the long-term evolution of the Integrated Public Alert and Warnings System (IPAWS) and WEA in concert with the evolution of hybrid commercial and government architectures for National Security and Emergency Preparedness communications. The advisory group would take these and other recommendations under advisement and use their program knowledge and subject matter expertise to select an affordable number of recommendations for further analysis. The most significant results of the selective analyses would be estimates of the level of effort and cost required to achieve clearly identified milestones. The information would be provided as a proposed Plan of Action and Milestones for a project to implement the recommendation or set of recommendations under analysis. The advisory committee would then prioritize the results based on WEA program objectives and consultation with subject matter experts and make funding recommendations to senior leadership.

Section 1

INTRODUCTION

1.1 BACKGROUND

The Wireless Emergency Alerts (WEA) system was established by the Federal Communications Commission (FCC) in response to the Warning, Alert, and Response Act of 2006 to allow wireless service providers to send geographically targeted emergency alerts to their subscribers. Under Executive Order 13407, the Secretary of the Department of Homeland Security (DHS), in coordination with the Department of Commerce and the FCC, is responsible for implementing and administering the national public emergency alert system and ensuring that the President can alert and warn the American people in the case of an emergency. Within DHS, the Federal Emergency Management Agency (FEMA) is responsible for the implementation and administration of the Integrated Public Alert and Warning System (IPAWS). FEMA has established the IPAWS program office to develop and manage technologies and processes capable of accepting and aggregating alerts from the President, the National Weather Service (NWS), and state and local emergency operations centers, as well as delivering validated, geographically targeted emergency alerts and warnings through WEA.

IPAWS allows local, state, tribal, or Federal authorities to issue a single alert message for transmission over multiple available public alert and warning channels.[1] Multi-channel alert dissemination is an important national resource to increase the likelihood of warning and mobilizing the maximum number of citizens in the shortest time possible regarding an imminent danger. WEA is a new channel in IPAWS that augments other public alert and warning channels such as television, radio, the Internet, sirens, and public electronic highway signage.

WEA allows the delivery of a short alert message (90 characters or less) to mobile devices within a specific geographical area using cell broadcast. It offers several unique benefits that position WEA as a critical national utility for supporting public safety. The high cellular subscription penetration rate[2] in the United States, combined with rapid advancements in cellular and smart phone capabilities, has made cellular handsets an indispensable platform for public alerts and warnings. Today, many people rely on their smart phones for essential daily activities—from navigation, data and voice communication, and entertainment, to shopping and surfing the Web. These developments position cellular networks as the best channel to reach the maximum number of citizens in an affected geographical area in the shortest possible time.

[1] http://www.fema.gov/integrated-public-alert-warning-system

[2] http://www.ctia.org/advocacy/research/index.cfm/aid/10323

WEA also allows AOs to broadcast an alert message to people located within a specific geographic region.[3] Once fully implemented and used, this geo-targeting feature cannot be easily matched by other IPAWS channels. For example, television and radio networks do not have an infrastructure to support this level of geographic granularity. WEA geo-targeting flexibility would enable alerting authorities to tailor alert messages and directives for specific emergencies and geographical areas.

The Johns Hopkins University Applied Physics Laboratory (JHU/APL) has been engaged by the DHS Science and Technology Directorate (S&T) First Responders Group (through the Space and Naval Warfare Systems Command) to support the deployment of WEA and to investigate possible system enhancements. As part of this effort, JHU/APL developed a computer model of WEA and investigated system performance under certain simulation scenarios.[4] This document discusses the recommended system enhancements based on simulation results and other analyses of the system.

1.2 APPROACH

The recommendations presented in this document were developed using the results of a previous Computer Model and Simulation Results study and the engineering best practices for secure and highly reliable systems. The project team evaluated the existing WEA architecture, protocols, and functional components against the desired features of an alert and warning system, including delivery to a significant portion of the target population, short latency, high reliability, ability to convey sufficient information and instructions, and geographic targeting. Based on these analyses, the team developed various recommendations that would enhance WEA system performance. The implementation details of the recommended enhancements are not described in depth in this document, but are deferred for future consideration.

1.3 WEA REFERENCE ARCHITECTURE OVERVIEW

In December 2006, the FCC established the Commercial Mobile Service Alert Advisory Committee (CMSAAC) to recommend system critical protocols and capabilities for WEA. The CMSAAC consisted of representatives from state and local governments, Federally recognized Native American tribes, representatives of the communications industry (including wireless service providers and broadcasters, vendors, and manufacturers), and national organizations representing people with special needs.[5] In its recommendations, CMSAAC proposed the architecture for WEA as shown in Figure 1-1.[6] The Aggregator and Alert Gateway functionality shown in the figure is currently implemented as part of FEMA's IPAWS Open Platform for Emergency Networks (OPEN) system.

---

[3] The current requirement is to support county-level geo-targeting, but much smaller regions with any shape can be supported at the discretion of individual CMSPs.

[4] "Wireless Emergency Alerts: Computer Model and Simulation Results," July 2013.

[5] The full list of CMSAAC members is listed in "Notice of Appointment of Members to the Commercial Mobile Service Alert Advisory Committee; Agenda for 12 December 2006 Meeting", Public Notice, 21FCC Rcd 14175 (PSHSB 2006).

[6] "Commercial Mobile Alert Service Architecture and Requirements," 12 October 2007.

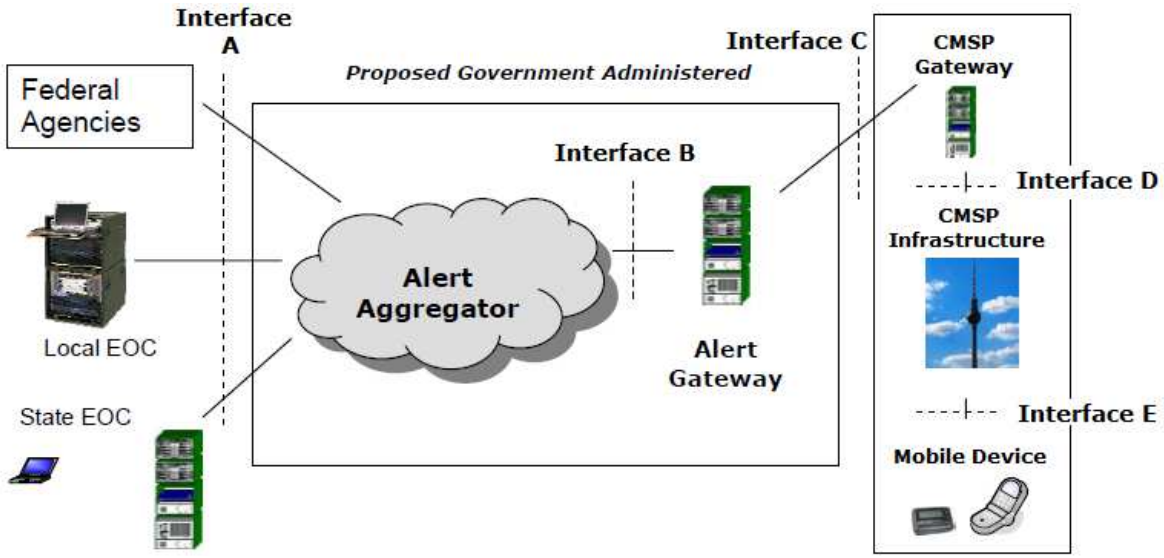


Figure 1-1 WEA Reference Architecture

At a high level, the following actions take place under this reference model:

- Alert Origination Systems (AOS) at the local, state, and Federal levels generate emergency alert messages for WEA using a data standard called the Common Alerting Protocol (CAP). These messages are transmitted to the Aggregator via Interface A.

- The Aggregator receives, authenticates, and aggregates emergency alerts from the AOS's and forwards them to the Federal Alert Gateway.

- The Federal Alert Gateway generates a Commercial Mobile Alert Message (CMAM).

- Based on CMSP profiles maintained in the Federal Alert Gateway, the Federal Alert Gateway delivers the CMAM over Interface C to gateways maintained by the appropriate CMSPs.

- The CMSP Gateway is responsible for formulating the alert in a manner consistent with the individual CMSP's available delivery technologies, mapping the alert to the associated set of cell site transceivers, and handling congestion within the CMSP infrastructure. WEA messages are transmitted using the Cell Broadcast Service (CBS) over-the-air interface.

- Finally, the alert is received on a customer's mobile device. The major functions of the mobile device are to authenticate interactions with the CMSP infrastructure, monitor for WEA messages, maintain customer options (such as the subscriber's opt-out selections), and activate the associated visual, audio, and mechanical (e.g., vibration) indicators that the subscriber has chosen as alert options.

Section 2

RECOMMENDATIONS

2.1 INTRODUCE MULTI-LEVEL PRIORITY

WEA currently treats all alerts, except Presidential alerts, with equal priority. Having additional priority levels would allow WEA to support processing of time-critical alerts (e.g., earthquake and tornado warnings) before other less-time-critical alerts. This would reduce latency for time-critical alerts if a WEA network element experiences congestion caused by excessive numbers of messages or commercial cell broadcast traffic.

2.1.1 RATIONALE

WEA uses two priority levels for all alert and warning messages. The high-priority level is used exclusively for Presidential alerts, and the low-priority level is shared by all other types of alerts. Current implementations of WEA components such as the Federal Alert Gateway and CMSP Gateway typically have two logical queues that correspond to the two priority levels, as illustrated in Figure 2-1. The processing of the Presidential queue takes priority over the processing of the non-Presidential queue. Messages within each queue are processed on a First-In First-Out (FIFO) basis. In the example in Figure 2-1, the non-Presidential queue has three alerts waiting for dispatch: a Tropical Storm Warning, a Tropical Storm Update, and an Earthquake Warning. In this example, any Presidential alert would be processed by the message dispatcher first, followed by the Tropical Storm Warning, the Tropical Storm Update, and then the Earthquake Warning, in this order.

Using one logical queue to process all of the non-Presidential messages on a FIFO basis can delay a more time-sensitive message (such as the earthquake warning). An earlier WEA simulation study[7] showed that queuing and processing delays can be significant when there is relatively high IPAWS traffic load or high cell broadcast traffic. Using multiple priority levels would reduce queuing delays in these cases.

[7] "Wireless Emergency Alerts Computer Model and Simulation Results," July 2013.

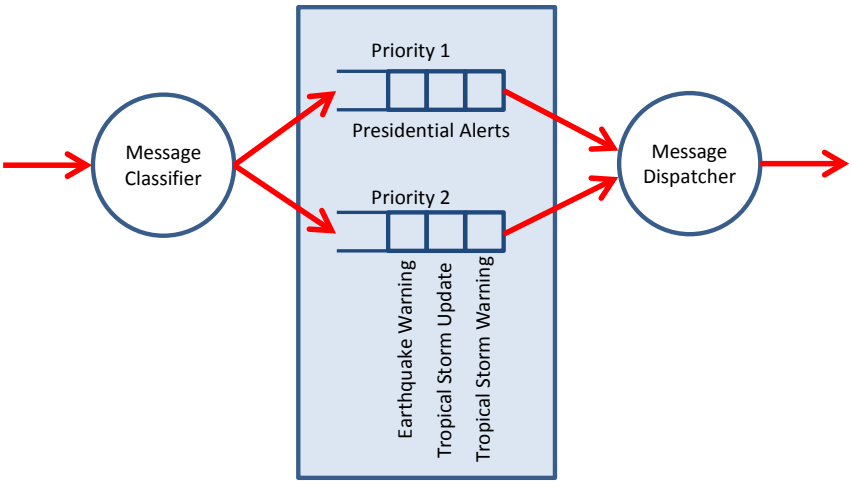


Figure 2-1 Logical Queues with Current Message Prioritization

2.1.2 RECOMMENDATION

Using a Multi-Level Priority (MLP) scheme and implementing Multi-level Priority Queuing (MPQ) is recommended to enable the timely delivery of the most critical messages. In this scheme, Presidential alerts still have the highest priority, but other alerts are assigned one of multiple priority levels according to a defined policy. Alerts at the same priority level have their own queue, and they are processed before queued alerts at lower priority levels.

Figure 2-2 illustrates the main functional components of the proposed MLQ implementation with three priority levels. Incoming messages are classified into one of three levels. Classification rules are established and can later be modified by a Policy Manager, which is a functional component of the system. Another functional component, the Message Classifier, evaluates multiple fields within each message (e.g., type, category, urgency, severity, certainty, event type) and uses the configured policy rules to assign a priority level to each message. Messages are then placed into different queues and serviced according to their priority level. For example, an earthquake warning can be placed into the Expedited Processing queue shown in the figure and processed before any messages within the Normal Processing queue. Messages in the same queue are processed in a FIFO fashion, as in the current implementations.

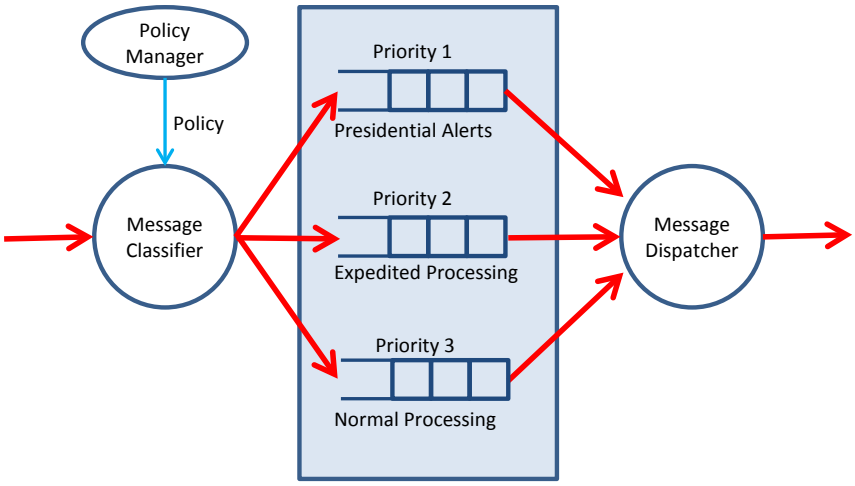


Figure 2-2 MLQ with Three Priority Levels

Message classification can be done at each WEA component independently according to message queuing capabilities and the specified policy. Alternatively, it can be done only at a single component (the AOS or the Aggregator), and the assigned priority can be written into a new field of the message and carried into the CMSP infrastructure. The first approach can be implemented independently by FEMA and individual CMSPs without a major standardization effort. The second approach requires standardization of a new message priority field, but it would be more efficient than the first approach. The second approach would also require less effort from CMSPs to implement.

2.1.3 EXPECTED BENEFITS

Implementing multiple priority levels for non-Presidential WEA messages would support processing of time-critical alerts (e.g., earthquake and tornado warnings) before other less-time-critical alerts. This can reduce the latency of the time-critical alerts when WEA network elements experience congestion caused by excessive number of messages or commercial cell broadcast traffic.

2.2 IMPLEMENT MANAGEMENT PLANE SERVICES AND PROTOCOLS

The functionality of telecommunication networks can be separated into three "planes." The data plane processes and forwards regular traffic for end-user applications; the control plane is responsible for controlling how the packets will be forwarded between nodes; and the management plane provides capabilities for managing and monitoring networked devices and the associated applications. Defining and implementing a WEA management plane would allow various new end-to-end system management services beyond the management capabilities that currently exist only within each WEA component. This would potentially require amendments to some existing WEA standards such as CAP v1.2,[8] J-STD-101,[9] and ATIS 0700006A.[10]

[8] OASIS, Common Alerting Protocol v1.2, "USA Integrated Public Alert and Warning System Profile, Version 1.0," October 2009.

[9] J-STD-101, "Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification," October 2009.

2.2.1 RATIONALE

The management plane is an essential functional element for managing and monitoring system status and performance. Management plane functions include collecting, aggregating, and displaying statistics to provide system administrators with sufficient visibility into the current performance and status of their system. Current WEA standards lack dedicated interfaces and protocols to support robust management plane functions. Whereas WEA protocols define the data and control plane functions necessary to support WEA capability, end-to-end management functionality is not supported. This is mainly because of the system-of-systems nature of WEA, where various components are the responsibility of various entities. System management is implemented independently within each WEA component (i.e., AO, IPAWS-OPEN, and CMSP systems), with minimal information sharing between components.

Without end-to-end management functions and interfaces, there are no adequate mechanisms in place that would allow AOs to obtain various types of important information. For instance, participating CMSPs can support different levels of geo-targeting granularity for WEA, and currently there are no mechanisms to convey the actual cellular footprint and boundaries of a target area to AOs. Consequently, AOs do not have an exact picture of where the alert will be delivered beyond an approximate granularity of Federal Information Processing Standard (FIPS) code boundaries (counties and county equivalents).

Similarly, there are no existing mechanisms to provide detailed status of issued alerts back to the AOs. WEA is a one-way broadcast system without any end-to-end confirmation of alert delivery. AOS's receive an acknowledgment of alert message validation by the Aggregator, and the Aggregator receives an acknowledgment of alert message validation by each CMSP Gateway. However, there is no mechanism for a CMSP to provide the Aggregator or the AOS with an acknowledgment of successful broadcast of an alert.

Finally, there are no mechanisms in WEA that inform the AOs about system performance statistics, such as the number of received and delivered alerts, the frequency of error conditions, and system availability.

Defining and implementing a management plane to provide this type of information would enhance the WEA user experience for AOs and enable them to better utilize the cellular infrastructure for public alerts.

2.2.2 RECOMMENDATIONS

Defining an explicit end-to-end management plane and related protocols would allow the implementation of new applications and services. Three recommended services can be implemented by a management plane:

- *Recommended Service #1: Introduce the ability for AOs to query and evaluate the actual cellular footprint and boundaries of a target area.* This recommended service would introduce applications with rich graphical user interfaces (GUIs) that allow AOs to view the actual cellular footprint of the target areas for each participating CMSP. With this new functionality, an AO could query for a target area and wait for a layered map to be displayed in response. This would require the Aggregator to receive the query from the

[10] ATIS 0700006A, "CMAS via GSM/UMTS Cell Broadcast Service Specification."

AOS, send a query to each participating CMSP over a new dedicated management plane interface, collect responses from the CMSPs, and return the aggregated responses to the AOS. The target area query problem is discussed in more detail in Appendix A.

Alternatively, the footprint discovery phase could be initiated proactively on a periodic basis (to discover any changes in CMSP capabilities), and the latest available information would be used at alert generation time. In this case, a database would be maintained by the Aggregator to support the proposed geo-targeting coverage discovery, thus eliminating the need to query all CMSPs at alert generation time. This capability would be useful for AOs to learn exactly where the alert will be delivered before pressing the Send button. They can fine-tune the target area before sending an alert to maximize the alerted target population, while minimizing sending alert messages to subscribers outside the desired target area.

- *Recommended Service #2: Provide a feedback loop.* A new management function can create a feedback loop based on a network of WEA broadcast sensors to verify an alert broadcast. Various WEA sensors can be deployed in each county that have the capability of receiving WEA messages from the major CMSPs serving that county. When a WEA message is broadcast by one of these CMSPs in that county, the sensors would receive the message and relay this information to the Aggregator over a new management plane interface. The Aggregator would, in turn, make this information available for AOS's.

  As an alternative to sensors, smart phones carried by various officials, such as police officers and emergency responders, can be programmed to relay the reception of WEA messages back to the Aggregator using the new management interface. The new capability would facilitate the confirmation of alerts delivered to the public and provide better measurement and analysis of WEA system behavior.

- *Recommended Service #3: Provide access to periodic federated reporting of segmented and end-to-end performance metrics.* A new management plane application would enable the collection and segregated delivery of various types of statistical data for each authorized AOS. This application would act as a repository for performance statistics. The Aggregator would collect various performance metrics, generate periodic status reports for AOS's, and make these reports available over the new management plane interface. Table 2-1 presents some sample metrics that can be captured and reported.

Table 2-1 Sample Metrics

Interface A Metrics	Interface C Metrics
Alert Messages Received	Transmission Control Cease Messages Received
Update Messages Received	Transmission Control Resume Messages Received
Cancel Messages Received	Link Test Messages Received
Test Messages Received	Acknowledgement Messages Received
Acknowledgement Messages Sent	Malformed Acknowledge Messages Received
Alerting Organization IP Addresses	TCP Session Connection Failures
TCP Session Connection Failures	IPSec Session Connection Failures
TLS Session Connection Failures	Interface Availability

Message WSDL Failures Received	Average Interface Latency
CAP v1.2 Message Failures Received	
Alert Message Errors Sent	
Test Message Errors Sent	
Certificate Name-Match Failures Received	
Interface Availability	
Average Interface Latency	

IP – Internet Protocol, IPSec – Internet Protocol Security, TCP – Transmission Control Protocol, TLS – Transport Layer Security, WSDL – Web Services Description Language

2.2.3 EXPECTED BENEFITS

Implementing management plane services would enhance the WEA user experience for AOs. This would enable them to assess system performance, plan their usage of the system, and better utilize existing capabilities of the cellular infrastructure for public alerts.

2.3 USE OPTIMIZED WEA BROADCAST REPETITION INTERVALS

Participating CMSPs retransmit WEA messages to maximize the number of users in the targeted area who receive the message. However, there is a tradeoff between cell broadcast resource usage by the retransmissions and alert reception latency. Optimizing the interval for retransmissions would reduce the load on cellular broadcast channels while ensuring that the greatest number of cellular devices will receive alert messages in the shortest amount of time.

2.3.1 RATIONALE

WEA uses CBS to deliver alerts and warnings to the public. Cell broadcast is a one-way, best-effort service that does not guarantee message delivery or provide acknowledgments of reception. Cellular devices may fail to receive a cell broadcast message for many reasons, including poor reception, interference, and handset status. In particular, when a cellular device is involved in a voice call, it does not process the cell broadcast channel. As a result, it would miss any WEA message transmitted while engaged on a call. WEA relies on broadcasting each message multiple times (repetitions) to reach those mobile devices that may have missed previous broadcasts.

The WEA repetition process consists of broadcasting the same WEA message multiple times based on two configurable parameters: the total number of broadcasts and the repetition period. The corresponding values associated with these parameters impact the system performance in terms of the percentage of the population successfully receiving an alert and the latency associated with its delivery. In a previous WEA simulation study,[11] the results demonstrated that a significant proportion of handsets receive an alert only after several repetitions because of ongoing phone calls. For this reason, setting the repetition period too large will introduce substantial delays in alerts. On the other hand, setting it too small will consume a lot of cell broadcast channel capacity, which is limited and shared among other WEA and non-WEA broadcasts. Setting the repetition period too small will also consume a lot of handset battery power and diminish the effectiveness of repetitions because multiple repetitions would be missed by an ongoing phone call.

[11] "Wireless Emergency Alerts Computer Model and Simulation Results," July 2013.

2.3.2 RECOMMENDATIONS

Developing a methodology for deriving the optimal values for the alert repetition process would minimize latency and maximize the alerted population percentage without excessive cell broadcast resource usage. The optimal parameter values for alert repetition are a function of the voice call characteristics, and these characteristics can vary in space (such as urban vs. rural areas) and time (day vs. night or weekday vs. weekend). In addition to using the conventional periodic repetition with a constant period, allowing the period to change from one repetition to another may also bring additional performance benefits.

CMSPs would store the optimal repetition parameters for various voice call characteristics in a simple lookup table. They would then use these tables with the hourly or daily call statistics from their networks and configure their WEA service with optimal repetition parameters. The lookup tables would be developed using analytical models, verified by simulation studies and experiments, and perhaps ultimately included in industry standards.

2.3.3 EXPECTED BENEFITS

Using optimized intervals for alert retransmissions would ensure that the greatest number of cellular devices will receive alert messages in the shortest amount of time, without overusing cell broadcast resources (such as transmission bandwidth and handset battery power).

2.4 INCREASE INFRASTRUCTURE RESILIENCE

The resilience of the WEA infrastructure against failures of system components can be increased by supporting backup communication channels or backup data centers. This would increase system availability during and after major disasters.

2.4.1 RATIONALE

Many types of natural and manmade disasters can damage various WEA components, including the communication network. However, WEA is expected to remain operational during and after such disasters. For instance, although a hurricane may damage some of the network infrastructure, cell towers, and data centers, there may still be urgent needs for sending new public alerts to the area regarding potential flooding, fires, and so forth.

2.4.2 RECOMMENDATIONS

Adding redundant components and communication channels to WEA can increase its resilience against such damages, so that there is a significantly higher chance that WEA remains operational in a disaster area. There are three recommendations for increased resilience:

- Multiple Internet Service Provider (ISP) support
- Public Safety Broadband Network (PSBN) support
- Distributed Data Center Architecture

The first two recommendations should be considered as alternatives to each other, whereas a Distributed Data Center Architecture can co-exist with and complement the first two.

- *Recommendation #1: Use multiple ISPs for Interface A.* Internet connectivity of a state or local AOS would typically use a single ISP. If this ISP experiences infrastructure damage and therefore ceases service in a disaster area, the AOS will not be able to issue any further alerts. One way to mitigate this would be to support two ISPs. During normal operation, an AOS would use just one of the two ISPs. If this ISP experiences service disruptions from damage or another reason, the AOS would be able to send alerts using the second ISP.

  Alternatively, a local jurisdiction may opt to rely on alert origination resources of adjacent jurisdictions or state-level resources to act as backup. This approach would allow local jurisdictions to avoid additional costs associated with multiple ISP subscriptions. However, adjacent jurisdictions must subscribe to different ISPs to have redundancy, and the necessary authorizations must be in place to allow different jurisdictions to originate alerts and warnings on behalf of others.

  Resilience against failures can be further increased by the multiple ISP approach if two ISPs serving an AOS employ different transport technologies. For instance, one ISP can have a terrestrial network, whereas the second ISP might have a satellite network. This would minimize the chances that both ISPs would fail simultaneously.

  The same approach can also be applied to IPAWS-OPEN, so that IPAWS-OPEN uses two different ISPs for connectivity. IPAWS-OPEN has two data centers, each of which is connected to all AOS's and all CMSPs. If each data center uses a different ISP for connectivity, WEA would remain operational for as long as at least one of these two ISPs is operational.

- *Recommendation #2: Use PSBN for Interface A.* The Middle Class Tax Relief and Job Creation Act of 2012 created the First Responder Network Authority (FirstNet) as an independent authority within the National Telecommunications and Information Administration (NTIA) to establish a single nationwide, interoperable PSBN.[12] If WEA Interface A support is built into the PSBN, AOS's and the IPAWS Aggregator can implement PSBN interfaces and use PSBN for WEA Interface A communications. An ISP can still be used as a backup channel for added resilience.

- *Recommendation #3: Implement a distributed architecture by regional data centers.* The current WEA architecture uses a centralized topology, where all WEA messages pass through one or two IPAWS-OPEN data centers. It is known that distributed topologies have better resilience against failures than centralized systems in general. Therefore, the resilience of WEA can be increased by implementing a distributed system architecture with multiple regional data centers. This would incur increased costs and more complex distributed data processing.

  A notional architecture of the recommended distributed architecture is shown in Figure 2-3. AOS's can send alert messages either directly to IPAWS-OPEN data centers, or to an available regional data center. Regional data centers would have similar functionality with IPAWS-OPEN, but less alert handling capacity. During normal operation, the regional data centers aggregate the alerts they receive and forward them to an IPAWS-OPEN data center. However, if the two IPAWS-OPEN data centers are down,

[12] http://www.ntia.doc.gov/category/firstnet

a regional data center can establish Interface C connections with CMSP gateways and send its messages directly to the CMSPs. Conversely, if a regional data center goes down, then AOS's connected to that regional data center send their alerts directly to an IPAWS-OPEN data center or to another regional data center.

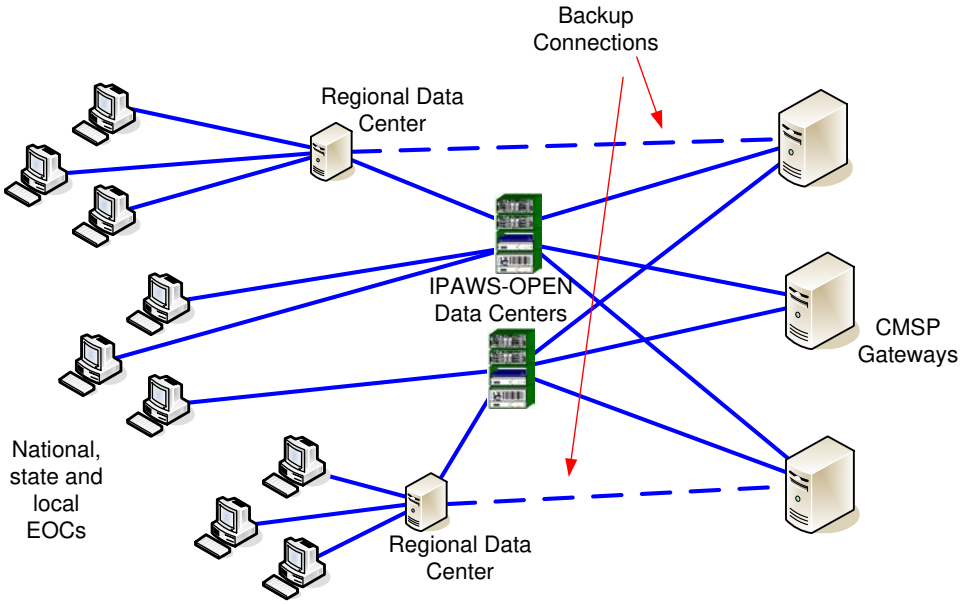


Figure 2-3 Notional Architecture of the Distributed Architecture

2.4.3 EXPECTED BENEFITS

Improving the resilience of the WEA infrastructure would increase system availability during and after major disasters.

2.5 IMPLEMENT MUTUAL TRUSTWORTHY PLATFORM VERIFICATIONS

Using information assurance standards from the Trusted Computing Group (TCG) (an international industry standards body formed to develop and promote open specifications for trusted computing and security technologies) and the National Institute of Standards and Technology (NIST) would allow verification of the integrity of software running on computer platforms at AOS's, the IPAWS Aggregator, and CMSP Gateways. This would ensure systems are in a trustworthy state and comply with Information Assurance (IA) guidelines for WEA operation. Such assurance would mitigate the potential transmission of false alerts by malicious software.

2.5.1 RATIONALE

Cyber attacks over the Internet continue to increase in both frequency and sophistication, as new vulnerabilities in all operating systems and widely deployed applications are exploited by hackers.[13] Moreover, these vulnerabilities are being used today to mount targeted attacks on specific

[13] "Internet Crime Complaint Center (IC3) 2011 Internet Crime Report," http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf.

organizations and systems on a regular basis. Because WEA is a critical channel for national public alert dissemination and is capable of reaching a very large number of people nationwide, it could be an attractive target for cyber criminals. Hackers may exploit WEA capabilities for financial gain, to cause chaos, or to attain publicity for special agendas.

WEA employs secure communication protocols and digital signatures to ensure the authenticity, integrity, and confidentiality of alert messages during transmission. However, unless the devices at both ends of the communication channels are guaranteed to be free of any malware, these communication protocols are not sufficient to ensure authenticity and integrity. If one of the peer devices is compromised, private cryptographic material such as keys and certificates on that device can be used to access the secure communication channels or to issue false alert messages.

The critical components of WEA are controlled by different administrative domains. Currently, there are no guarantees that common best security practices and proper IA policies are applied across these independent domains. The security of the entire WEA system is only as strong as its weakest component. Once a WEA node is compromised by an attacker, it may be used to infect and gain control of other WEA nodes.

A mechanism to assess and verify the integrity of individual systems is required to ensure overall security of WEA.

2.5.2 RECOMMENDATION

This recommendation proposes to enforce standard IA technologies and specifications over the entire WEA system by establishing trust between individual components. Trust establishment requires integrity measurements of all inter-administrative-domain computing platforms. Assessing the integrity of each computer involved in any WEA transaction is essential to allow proper identification of each device, to establish trust relationships between devices, and to secure the end-to-end system.

Trusted Network Connect (TNC), developed by TCG, is an open industry standard architecture defined primarily to support network access control.[14] [15] TNC specifications define an open and extensible architecture to allow the integration of computer security tools from independent vendors.

The TNC architecture uses integrity measurements collected from any computing device that needs permission to access a local or a remote network. These measurements are monitored by a Policy Decision Point (PDP), which assesses the integrity of the computing devices and either allows or prevents access.

In the recommended solution, TNC standards will be implemented in AOS's, the IPAWS Aggregator, and optionally in CMSP Gateways. AOS's will perform integrity measurements and send this information to the PDP function at the IPAWS Aggregator. The PDP will then decide whether the AOS can be trusted, and make the access decision accordingly. Similar functions can also be implemented over Interface C, between the IPAWS Aggregator and the CMSP Gateways. To avoid alert message processing delays, these measurements and exchanges should not take place

[14] "Trusted Computing Group (TCG) Federated Trusted Network Connect (TNC) Specification," Version 1.0, Revision 26, 18 May 2009.

[15] "Trusted Computing Group Trusted Network Connect (TNC) Architecture," Version 1.1, May 2006.

prior to processing each alert transaction. Instead, the TNC-based trust should be established during initial session setup, and then reestablished periodically to maintain the trust relationship.

Using the TNC architecture to establish mutual trust will provide mechanisms to ensure WEA components are effectively managed to comply with the requirements and guidelines of the Federal Information Security Management Act.[16] Determination of when to grant and maintain trust relationships between WEA components can be based on NIST recommendations for security controls on Federal Information Systems and Organizations.[17]

2.5.3 EXPECTED BENEFITS

Verification of the integrity of software running at AOS's, the IPAWS Aggregator, and CMSP Gateways would ensure the systems are in a trustworthy state. This would protect the systems against potential transmission of false alerts by unauthorized parties.

2.6 ENHANCE THE ACCURACY OF GEO-TARGETING

The geo-targeting precision of WEA can be improved beyond the cell site or cell sector granularity that is possible today. Limited geo-targeting precision can cause portions of the public to receive irrelevant alerts or to miss relevant alerts. Several enhancements to geo-targeting would minimize the occurrence of both of these events. The recommended enhancements rely on broadcasting alerts to an area wider than the affected area and making use of the location awareness of mobile devices, so that a user is notified of an alert only if the mobile device is inside the affected area. Broadcasting alerts to a wider area would prevent missed alerts caused by geo-targeting inaccuracy, whereas using device location awareness would minimize geographically irrelevant alerts. The resulting performance improvements would encourage more widespread adoption of WEA by emergency managers and the public.

2.6.1 RATIONALE

The current WEA implementation has significant limitations on the granularity of geo-targeting. For each WEA message, two mapping steps determine the actual alerted area. The first step is to specify the affected area by one or several area descriptors of a CAP message. These area descriptors are also copied to the area descriptors of a CMAM and passed to the CMSP Gateways. Whereas WEA protocols allow using FIPS codes (counties, and county equivalents) as well as geospatial shapes such as polygons and circles to describe the affected area, the only mandatory requirement is for the use of FIPS codes. For many emergency scenarios, this mapping does not provide sufficiently fine granularity. For instance, although the affected area may be a small part of one county, or a small area at the boundary of multiple counties, the entire county or counties would be alerted. Some issues and potential solutions related to sub-county alerting by geospatial shapes were discussed previously in Subsection 2.2.2.

The second mapping is within the CMSP infrastructure to translate the specified area in the CMAM into a cell broadcast area described by a set of base stations. The actual alerted area is determined by the radio frequency (RF) coverage of all base stations selected to transmit the alert message. The degree of granularity of this second mapping is unavoidably limited by the size of the

[16] H.R. 2458-48, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

[17] NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," Revision 3, August 2009.

area covered by individual cells. An exact match between the RF coverage of all the selected cells and the affected area specified in the CMAM is highly unlikely, and the result is typically a coverage spillover whereby the RF coverage of the selected cells extends beyond the designated affected area.

Increasing the accuracy of WEA geo-targeting to areas with any size and shape would minimize the potential for public confusion caused by irrelevant alerts and encourage more widespread adoption of WEA by AOs by building trust.

2.6.2 RECOMMENDATION

There are three main mechanisms that can potentially be used by WEA to convey the affected area information to the public:

- Broadcast the message to the smallest possible area that covers the affected area, and let the individual mobile devices alert users whenever they receive a new message. This is how WEA currently operates. Recipients of a message assume they are in the affected area, but they may actually be outside the area because of coarse geo-targeting granularity.

- This option is the same as the first, but also includes a text description of the affected area in the message. In this case, recipients can determine whether they are in the affected area by reading the message. The main problem with this option is the 90-character limitation of WEA messages. It would be difficult or impossible to sufficiently describe an area and provide other essential information within 90 characters.

- Include a coded (non-text) description of the affected area as non-displayable information within the WEA message, broadcast the message to an area that fully covers the affected area, and let the mobile device determine whether to alert the user, based on their current location. This option is the recommended solution.

In the recommended solution, each alert message broadcast includes a description of the affected area in its header. The message is broadcast to an area that encompasses the entire affected area. This would require passing the geographic information included in a CMAM all the way to the mobile devices. Once a mobile device receives the message, it compares its current location with the affected area coded in the message header and reacts in one of two ways:

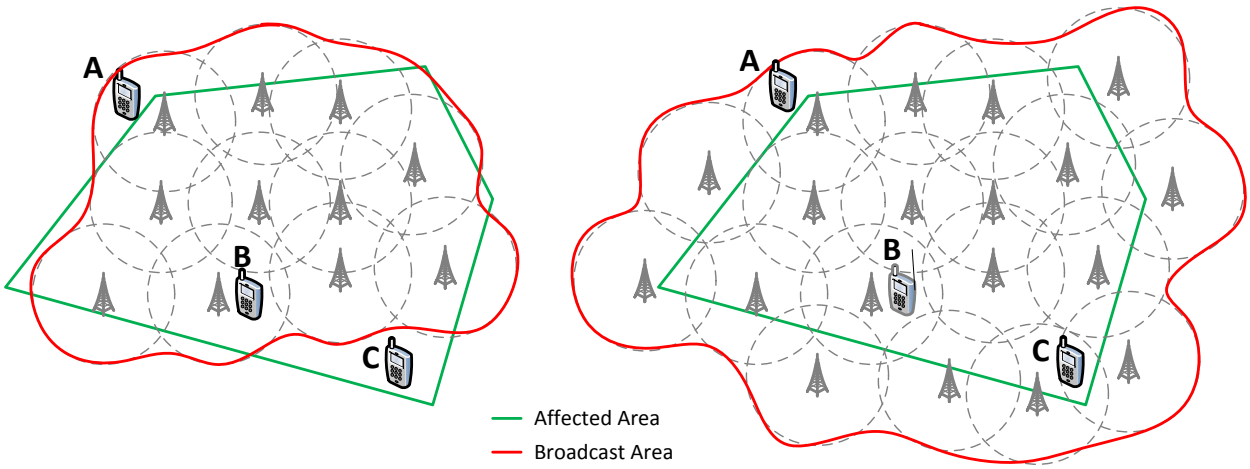
- If the current location is within the affected area, the mobile device alerts the user and displays the message text.

- If not within the affected area, the device stores the message internally but does not generate any indication to the user. If the mobile device enters the affected area later, it alerts the user and displays the stored message text.

Figure 2-4(a) depicts geo-targeting in the existing WEA system. WEA messages are broadcast to an area that approximates the affected area. For example, a simple and common method for determining the broadcast area is using only the set of cell towers inside the affected area. Handsets inside the broadcast area that receive the WEA message alert the user. However, because of the mismatches between the affected area and the broadcast area, some handsets in the affected area may not receive the alert, while some handsets outside the affected area receive the alert. In

Figure 2-4(a), Handset A is outside the affected area but can receive the alert because it is inside the broadcast area; however, Handset C cannot receive the alert although it is inside the affected area.

Figure 2-4(b) depicts the recommended solution, where WEA messages are always broadcast to an area that is larger than the affected area. In the recommended solution, the handsets that receive a WEA message decide whether to alert the user, based on the user's location. In Figure 2-4(b), all three handsets receive the WEA message and compare their location with the affected area. Handsets B and C alert the user because they are inside the affected area, but Handset A does not.



(a) Existing WEA System **(b) Recommended Solution**

Figure 2-4 A Comparison of Broadcast Areas in Existing WEA System and in the Recommended Solution

An important characteristic of this approach is that the broadcast area no longer needs to exactly match the affected area specified by the AO; it suffices that the broadcast area fully covers the affected area. The exact boundary of the affected area is now passed to the mobile device, which determines whether it is located in the affected area.

The recommended solution requires mobile devices to have the capability of obtaining location information. This is not expected to be a serious limitation over the longer term because smart mobile devices are becoming more and more widespread every day. Smart mobile devices can typically obtain location information using global positioning system (GPS), triangulation based on signal reception, or an indoor positioning system. Because these operations drain battery power, mobile devices can check their locations at regular intervals instead of continuously. When a mobile device receives a WEA message, it can use its last known location to determine whether to alert the user. Alternatively, reception of a WEA message can trigger a location update on the device, increasing accuracy. Updating location only after receiving a WEA message would conserve battery power, but would introduce additional delay before an alert is displayed to the user. Older-generation devices that do not support the recommended functionality would simply display every received alert, as in the current practice, though they may display more alerts due to larger broadcast areas. The recommended solution also requires protocol changes to support inclusion of area information in cell broadcast message headers as previously described.

2.6.3 EXPECTED BENEFITS

Enhancing the geo-targeting accuracy of WEA would reduce missed alerts and over alerting. This is expected to encourage more widespread adoption of WEA by emergency managers and the public.

2.7 UTILIZE GEOGRAPHICAL EMERGENCY AFFINITY SUBSCRIPTIONS

This functionality would allow the public to receive WEA messages broadcast for a specific geographical area, while being at locations outside that area.

2.7.1 RATIONALE

As WEA penetration increases over time, its deployment and use in actual emergencies reveals potential shortcomings that need to be addressed to encourage participation by emergency managers and their user populations. WEA was used when Hurricane Sandy struck the U.S. East Coast in late October 2012. Several emergency messages were issued for blizzard warnings, flood warnings, and evacuation notifications in various locations along the East Coast. Although WEA was successful overall during the storm, some commentators expressed concern that "individuals who may be from the East Coast but were not physically in the storm-affected areas when alerts were being sent would not have received the messages."[18]

The desired functionality is that individuals should be notified when an alert message is issued to their home area even if they happen to be outside that area at the time the alert message is broadcast. WEA could be enhanced with this capability as described in the next section.

2.7.2 RECOMMENDATION

Figure 2-5 depicts the recommended solution. For a given emergency event, the associated alert message can be targeted to a subset of the population that belongs to one of the following categories:

- People physically present in the affected area, often directed to take some action, here called "affected individuals."
- People who were present in the affected area when an initial alert was issued but later relocated, possibly as directed by the initial alert. Here they are called "relocated individuals." Ideally, relocated individuals would receive updates to the initial alert.
- People outside the affected area who have an interest in the affected area, such as family, property, business relationships, or other responsibilities in the affected area. Here they are called "related individuals."

The recommended solution uses the same approach described for enhanced accuracy in geo-targeting (Section 2.6), based on location-aware smart mobile devices. When a WEA message is broadcast by a CMSP, it will be broadcast to an area wider than the affected area. The alert message will include a descriptor of the affected area in its header, and each mobile device will determine whether the alert is of interest to the user.

[18] http://www.govtech.com/public-safety/National-SMS-System-Successful-During-Superstorm-Sandy.html

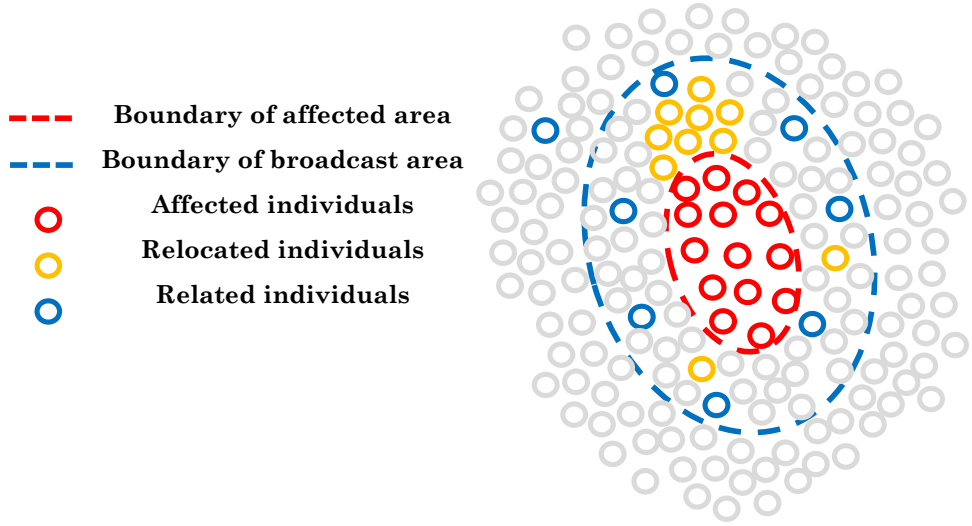


Figure 2-5 Illustration of Different Alerted Categories

The additional steps that would be required for the geographical affinity subscription capability are as follows:

- To enable alerting related individuals, users would have to configure their devices. They have to specify their locations of interest, which could be done through a user interface with a map on the device.

- When a message is received, the device would make a decision based on the current location, as well as the user-specified locations of interest.

This solution also supports alerting relocated individuals, as follows:

- When a device receives an alert while inside the affected area, it alerts the user and also stores the alert.

- If the device later moves outside the affected area but still receives an update to the initial alert (possible since a wider broadcast area is used), it recognizes this as an update to the earlier message and notifies the user.

Because the recommended solution requires the broadcast area of a message to be wider than the affected area, consideration must be given to the recommended size of the cell broadcast area relative to the affected area. Users will only receive related or updated alerts from inside the broadcast area. Choosing a wider broadcast area would potentially reach a larger number of users who expressed interest in the affected area or who moved outside the affected area. However, widening the broadcast area would increase the network-wide broadcast volume. Analysis is needed to assess whether this presents a serious concern and to determine a reasonable boundary for the broadcast area. Message prioritization can be used to give related alerts and updates a lower priority, so that they are broadcast only when cell broadcast capacity is available. If the analysis reveals significant challenges, a potential alternative solution would be to rely on subscription-based, non-broadcast mechanisms to reach the remaining concerned users.

2.7.3 EXPECTED BENEFITS

A Geographical Emergency Affinity Subscription would allow the public to receive WEA messages broadcast for a specific geographical area, even while at locations outside of that area.

2.8 POST-DISASTER WEA MODE

Implementing a new operational mode among CMSPs would allow continuity of the WEA service after a disaster. It would also facilitate emergency communications with the public via cellular devices using a temporary cellular infrastructure that can be deployed by first responders. The cellular infrastructure of one CMSP or the newly deployed temporary infrastructure would be used to send WEA alerts to subscribers of all CMSPs whose infrastructures have been damaged.

2.8.1 RATIONALE

WEA has inherent characteristics that make it more resilient than other emergency alert channels; it is likely to remain operational after a major disaster to disseminate alert and warning messages to the public. In particular, handsets are battery operated, which increases the likelihood that most will remain functional for some period after a loss of power. In addition, the geographically distributed deployment of cellular sites and associated infrastructure allows parts of the system to operate even if other parts experience failure. These features make WEA an attractive candidate channel for dissemination of new, lifesaving information about emergent dangers that may develop after the immediate incident.

Most CMSPs make major, continuing investments to improve the reliability and availability of their cellular networks. Nonetheless, major disasters will still potentially damage the cellular network and impact the ability to disseminate post-disaster WEA messages. For example, severe hurricanes and earthquakes can cause random physical destruction to cellular radio transmission equipment (cell site antennas or complete cell towers), which would cause coverage gaps for affected CMSPs. Subscribers to an affected CMSP would not receive new WEA messages in the gap regions even though some other CMSP might still have cellular infrastructure operating in those regions.

Figure 2-6 illustrates overlapping coverage of two CMSPs in one area. On the left, the entire area is getting service from both CMSP A (blue cells) and CMSP B (pink cells) before the disaster. On the right, CMSP B is shown to experience damage in the west side of the area, so cells X and Y are not functioning. Similarly, CMSP A is shown to experience damage in the east side of the area, so cells 1 and 2 are not functioning. Subscribers of CMSP B will experience the loss of WEA service in cells X and Y, even though these cells are partially covered by CMSP A; subscribers of CMSP A will experience the loss of WEA service in cells 1 and 2, even though these cells are partially covered by CMSP B.

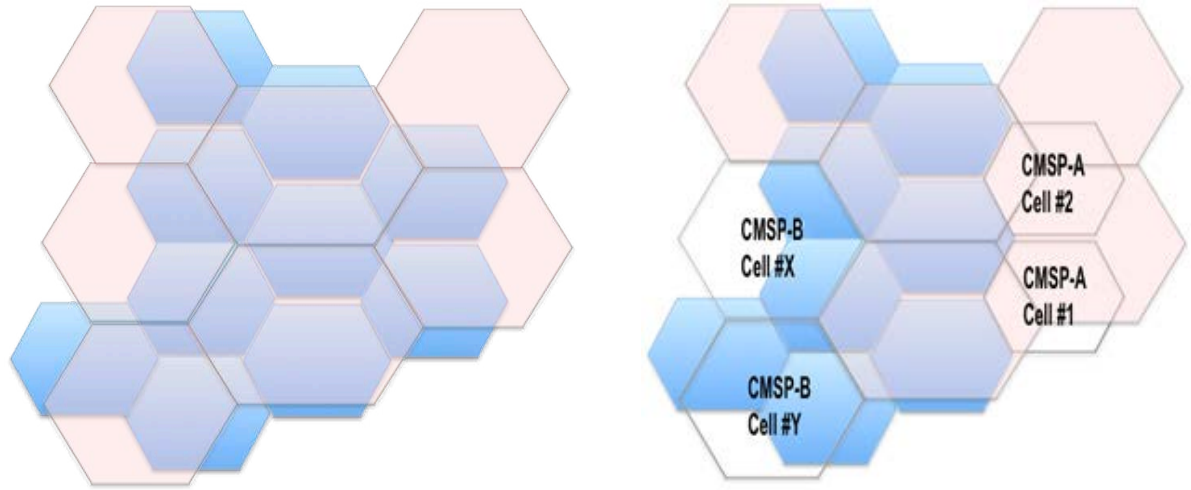


Figure 2-6 Cellular Coverage of Two CMSPs Before (left) and After (right) a Disaster

In other scenarios, all CMSPs providing service to a region may experience failure caused by infrastructure damage. This would especially be likely if several CMSPs in a region share cell towers. In this case the only way to send new emergency messages to the region would be to set up a temporary cellular infrastructure.

2.8.2 RECOMMENDATION

A new post-disaster mode of operation for cellular networks would enable subscribers to receive WEA messages from other CMSPs when the CMSP they subscribe to experiences service disruption. This mode could be activated on demand, enabled only after a major disaster or other event that causes cellular infrastructure damage to one or more CMSPs. The WEA post-disaster mode would guarantee that all WEA-capable mobile devices receive WEA messages as long as there is at least one operational CMSP in the area or if a temporary infrastructure is deployed in the affected areas.

The recommended solution requires cooperation among CMSPs after disasters to maximize the reception of additional WEA messages. It also requires the widespread use of cellular devices that can support multiple RF spectrum ranges and cellular protocols. This is not considered to be a significant hurdle because most mobile devices today are designed to support many legacy and new cellular protocols as well as international roaming. Unlike standard cellular roaming, mobile devices will not be able to originate or receive phone calls with the recommended solution, primarily because of the capacity limitations of cellular networks. Supporting higher numbers of subscribers during a disaster could reduce the performance of a network and therefore cause increased congestion. It is likely that CMSPs would be more amenable to accept the recommended solution if they receive assurance that their network will not experience additional load or potential loss of revenue caused by increased congestion.

The recommended solution would also facilitate the use of a temporary cellular infrastructure that can be deployed by first responders when the entire cellular infrastructure in an area is damaged. Setting up a temporary cellular infrastructure would require the availability of a limited

number of mobile radio transmitters with centralized controllers and cell broadcast functionality. Core network connectivity to the temporary transmitters could be provided by a satellite; other network alternatives are also feasible. These temporary systems would then be deployed at selected emergency areas to restore WEA service and to facilitate other emergency communications with the public via cellular devices.

WEA post-disaster mode does not introduce any traffic load to a given CMSP network from subscribers of other CMSPs because all WEA messages are transmitted as cell broadcasts. Each operational CMSP will continue to broadcast WEA messages regularly, with the addition of new admission control mechanisms that allow devices from other CMSP networks to receive these broadcasts.

In WEA post-disaster mode, mobile devices must always attach to and use their primary provider network when it is available. The primary provider network would remain the preferred network for all voice and data communications and for receiving WEA messages. If a mobile device is able to access its primary provider network, the control software in the mobile device would ignore signals from all other networks, even when these other networks have stronger signals. A mobile device will switch to the recommended post-disaster mode only when it is no longer able to reach its primary provider network or any network where it is authorized for roaming. When a mobile device determines that it should switch to the post-disaster mode, it would first find a serving network with WEA post-disaster mode enabled. It would verify the authenticity of the serving node and then register to be able to receive WEA messages from that network.

All WEA cell broadcast messages can be assigned globally unique identifiers in post-disaster mode. Then, the existing process for handling cell broadcast on mobile devices will ensure that repeated receptions of cell broadcast messages will be ignored, regardless of which CMSP tower transmits the alert.

Implementation of the recommended mode requires software upgrades on the mobile devices and in the cellular network infrastructure to support new authentication and registration operations. Authentication can be implemented similar to the Universal Mobile Telecommunications System (UMTS) mutual-authentication procedures,[19] but these procedures can be simplified because mobile devices are not required to provide regular voice and data communications in WEA post-disaster mode.

2.8.3 EXPECTED BENEFITS

Implementing the recommended post-disaster mode would allow continuity of WEA service after a disaster. It would also facilitate emergency communications with the public via cellular devices using a temporary cellular infrastructure that can be deployed by first responders.

2.9 INCREASE TEXT MESSAGE LENGTH

Currently, WEA messages are limited to 90 characters because of a requirement to use only a single "page" of cell broadcast for each message. Using multiple pages would allow longer messages, which can convey more information to the public.

[19] European Telecommunications Standards Institute Technical Specification (TS) 133 102, "3G Security, Security Architecture."

2.9.1 RATIONALE

The current 90-character limitation for emergency alerts, specified by the FCC,[20] restricts AO's ability to provide detailed information to the public in the event of an emergency. Mobile subscribers are advised to monitor other alert channels such as television or radio for more information about an alert, but this may not be possible due to lack of television or radio access, lack of power, or infrastructure outages. Restricting message size to 90 characters is not a cell broadcast limitation. Existing protocols would readily support longer messages if the FCC-imposed restrictions were removed.

2.9.2 RECOMMENDATION

Supporting messages longer than 90 characters would not require any changes to the Interface A or Interface C protocols. Arbitrary message lengths are already supported by the <parameter> element of the CAP messages and by the <CMAC_text_alert_message> and <CMAC_text_alert_message_length> elements of the CMAC messages. The only change required for these two interfaces would be amending the CAP IPAWS Profile[21] and the ATIS/TIA Commercial Mobile Alert Service (CMAS) Interface C Specification[22] to permit the use of longer messages.

WEA currently uses the automated 90-character message generation functionality implemented in IPAWS-OPEN. Various CAP fields are used to generate alert text instead of relying on an AO to enter free-form text. If message sizes are increased, this functionality would have to be modified to generate longer messages with more information.

WEA messages longer than 90 characters would require using multiple pages over the cell broadcast channel. Both Global System for Mobile Communications (GSM) and UMTS networks support multiple page cell broadcast, up to a maximum of 15 pages.[23] As a result, WEA messages up to 1350 characters can be supported by the existing standards. The only additional requirement for the CMSP infrastructure would be to separate long messages into multiple pages (1 to 15), none exceeding 90 characters.

2.9.3 EXPECTED BENEFITS

Increasing the WEA message length beyond 90 characters would allow more detailed information to be conveyed to the public.

2.10 ENHANCE MULTIMEDIA SUPPORT

WEA can be enhanced to support the delivery of alerts with audio and video content.

---

[20] 47 Code of Federal Regulations (CFR) Part 10, FCC 08-99, 22 September 2008.

[21] OASIS, Common Alerting Protocol v1.2, "USA Integrated Public Alert and Warning System Profile, Version 1.0," October 2009.

[22] J-STD-101, "Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification," October 2009.

[23] ATIS-0700007, "Implementation Guidelines and Best Practices for GSM/UMTS Cell Broadcast Service," October 2009.

2.10.1 RATIONALE

WEA currently relies on the cell broadcast service provided by CMSPs to deliver text alerts to the public on their cellular devices. More effective alerting would be achieved if the alert messages were enriched beyond simple text; in particular, if multimedia content was supported. Broadcasting an appropriate audio or video stream related to the emergency event could help the public better understand and deal with the emergency situation. Because the cell broadcast service currently offered by CMSPs is limited to text broadcast, an alternative would be needed to deliver multimedia content. This section addresses this need by exploring how a multimedia broadcast service could be made available for use by WEA when alerting the public.

2.10.2 RECOMMENDATION

Today's cellular multimedia delivery is based on unicast delivery, with users streaming stored video or live television in a client-server mode. In unicast delivery a separate point-to-point connection must be established and maintained separately for each recipient. This type of operation on the radio interface is practical for a small number of subscribers who stream audio or video content simultaneously. However, it does not scale as the number of subscribers increases, thus requiring many simultaneous connections to be established and maintained. This would generate a large amount of traffic on the air interface, where spectrum is a limited resource.

Studies have shown that it is more efficient to broadcast a video stream within a cell site when the total number of users simultaneously accessing the stream in the same cell is more than some threshold.[24] The capacity enhancing techniques developed for point-to-point communication (which is bidirectional) cannot be used for broadcast because the broadcast radio channel must serve multiple users simultaneously. In other words, the broadcast signal cannot be adapted to individual users and must always be strong enough for the mobile with the poorest radio quality. In contrast, unicast has associated uplink feedback and the radio resources can be tailored to the user's current channel conditions instead of the worst case.

Broadcast has a capacity advantage over dedicated point-to-point connections when many recipients are using the same cell. Because the audience of a WEA video alert would potentially be very large, broadcast would be the most appropriate delivery mode for WEA audio and video. Therefore, there is a need for point-to-multipoint delivery on the radio interface that can support broadcast services more efficiently. The Third-Generation Partnership Project (3GPP), which is the organization responsible for the GSM and UMTS standards, already addressed multimedia broadcast and multicast and developed the Multimedia Broadcast and Multicast Service (MBMS) standards specification.[25] MBMS introduces small changes to existing radio and core network protocols, which make mobile broadcast a relatively inexpensive technology to introduce. MBMS adds a set of functions that control the broadcast delivery under the term "broadcast service center" [equivalent to the cell broadcast center (CBC) for CBS] as well as channels for point-to-multipoint radio transmission within a cell. MBMS uses the General Packet Radio Service (GPRS) and Enhanced Data Rates for GSM Evolution (EDGE) packet data channel (PDCH) in GSM, and it uses the forward access channel (FACH) and the secondary common control physical channel (S-CCPCH) in UMTS. It uses multi-slot operation to set up a multimedia broadcasting channel in GSM, supporting up to five timeslots per MBMS session, and can achieve up to 256 kbps as a user bit rate.

[24] F. Hartung et al., "Delivery of Broadcast Services in 3G Networks," *IEEE Transactions on Broadcasting*, Vol. 53, No. 1, March 2007.

[25] 3GPP TS 22.146, "Multimedia Broadcast and Multicast Service (MBMS)," December 2011.

With today's device display size and resolution, 64 kbps is adequate for news and 128 kbps for sports applications, so video alerts are expected to be easily supported. MBMS is flexible. Within a cell site, a CMSP can configure some radio resources for a few MBMS channels (possibly with different bit rates) and use the remaining capacity for voice and unicast services.

There are a number of ways in which WEA can introduce multimedia content when alerting the public using MBMS:

- A video stream can be made to pop up on the screen of the mobile device in a way that is similar to the current text message alert.

- The multimedia message can be broadcast periodically and indicate its predetermined timing periodicity in the text alert.

- The multimedia message can be broadcast continuously during some time period, and the user could join the stream any time during that period.

There is a strong incentive for CMSPs to provide a multimedia broadcast service because video-streaming usage keeps increasing (e.g., due to mobile live television). The basic standards to provide multimedia WEA messages are available today, and it is recommended that WEA take advantage of this service by developing the required modifications to its interface protocols and use cases.

2.10.3 EXPECTED BENEFITS

Support for audio and video content in alerts would allow more detailed information about the situation and the required action to be conveyed to the public.

Section 3

CONCLUSIONS

The recommendations presented in this document involve a number of important technical, programmatic, and policy decisions that must be made or endorsed by the FCC, FEMA, DHS, CMSPs, the AO community, and state and local first responders. The success of the WEA service strongly depends on its adoption by the AO community and the public. The evolution of the WEA system must be coordinated to answer the needs of its users.

The DHS S&T WEA Program Management Office should work with NTIA and the FCC to establish a technically focused Advisory Group to guide the long-term evolution of IPAWS and WEA in concert with the evolution of hybrid commercial and government architectures for National Security and Emergency Preparedness communications. Additionally, DHS S&T and FEMA IPAWS coordination with the rollout of FirstNet for Public Safety Broadband Networks and the ongoing Department of Defense and FEMA work for National Senior Leadership communications provide opportunities for unity of effort that should not be ignored.

Such an advisory group would take these and other recommendations under advisement and use their program knowledge and subject matter expertise to select an affordable number of recommendations for further analysis. Subject matter expertise should include strong representation from state and local AOs and the public safety community. The analysis could be performed by the organizations making the recommendations or by third parties, as determined by the advisory board on a case-by-case basis. The most significant results of the selective analyses would be estimates of the level of effort and cost required to achieve clearly identified milestones. The information would be provided as a proposed Plan of Action and Milestones for a project to implement the recommendation or set of recommendations under analysis. The advisory committee would then prioritize the results based on WEA program objectives and consultation with subject matter experts and make funding recommendations to senior leadership.

Appendix A

TARGET AREA QUERY PROBLEM

WEA development mandated support for county-level geo-targeting. Implementing capabilities for geo-targeting areas smaller than county boundaries (i.e., capabilities to broadcast an alert only to a target area smaller than a county) was left optional for participating CMSPs. In the current implementation of WEA, a county-level target area specification, in the form of one or more FIPS codes, is always provided to CMSPs with each alert message. Optionally, a smaller target area can be specified in terms of a polygon, a circle, or a Geographic Names Information System representation in addition to the FIPS codes. If a smaller target area is also provided, and if a CMSP supports more precise geo-targeting than county boundaries, the CMSP will broadcast the alert only to that small target area; otherwise, the entire county is alerted.

Many CMSPs offer WEA to their subscribers, each with different coverage regions and different geo-targeting capabilities. Currently, there are no mechanisms in place to advise AOs on the geo-targeting capabilities of the participating CMSPs. Without such a mechanism to discover the geo-targeting capabilities of CMSPs in a given region, an AO knows only that all CMSPs support county-level geo-targeting but does not know the actual footprint of the target area. This prevents AOs from taking full advantage of available capabilities for finer-grained geo-targeting.

To illustrate this problem with an example, consider a hypothetical terrorist attack scenario, in which a civil warning is issued to the entire county. Further assume that once an initial assessment of the situation is made, authorities discover that a specific area of the county needs to be evacuated and that in another area people should take shelter. Figure A-1 illustrates the different target areas in this scenario.

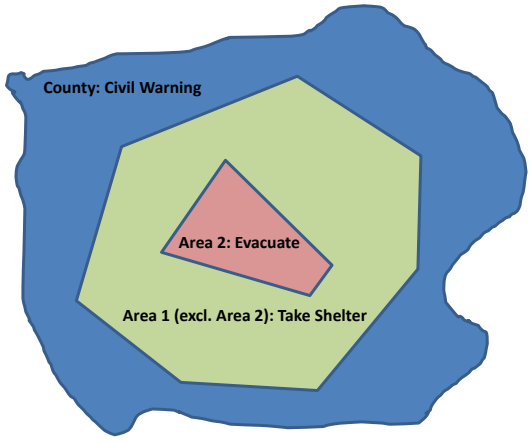


Figure A-1 Different Target Regions in a Hypothetical Scenario

WEA may not work well for this kind of sub-county alerting. The subscribers of a CMSP that supports only county-level geo-targeting would receive confusing and potentially conflicting messages in this scenario.

Table A-1 presents the different messages that would be received in each target area by a CMSP that supports sub-county–level geo-targeting and a CMSP that supports only county-level geo-targeting. Subscribers of the second CMSP will get all of the alerts issued in the county, not just the ones targeted for their sub-county area. In this example, subscribers to the second CMSP who are outside both Areas 1 and 2 unnecessarily receive the Evacuate and Take Shelter messages as conflicting instructions. Furthermore, subscribers to that CMSP who are inside Area 1 or Area 2 receive an Evacuate message followed by Take Shelter, which is conflicting. If the alerts contained free-form text to describe the relevant area, it may be possible to mitigate the confusion to some degree, but the description will have to conform to the 90-character limit of WEA.

Table A-1 Alerts Received in Different Target Areas with and without Sub-County Geo-Targeting Support

Target Area	CMSP with Sub-county–level Geo-targeting	CMSP with County-level Geo-targeting
County	Civil Warning	Civil Warning Take Shelter Evacuate
Area 1	Civil Warning Take Shelter	Civil Warning Take Shelter Evacuate
Area 2	Civil Warning Evacuate	Civil Warning Take Shelter Evacuate

A new management plane service is recommended to solve this problem, as described in Section 2.2. This service would allow querying a target area to learn its existing geo-targeting capabilities and the actual footprint of a WEA broadcast. This querying could be done either periodically or before sending each alert.

Appendix B

LIST OF ACRONYMS AND ABBREVIATIONS

3GPP	Third-Generation Partnership Project
AO	Alert Originator
AOS	Alert Origination System
CAP	Common Alerting Protocol
CBC	Cell Broadcast Center
CBS	Cell Broadcast Service
CMAM	Commercial Mobile Alert Message
CMAS	Commercial Mobile Alert Service
CMSAAC	Commercial Mobile Service Alert Advisory Committee
CMSP	Commercial Mobile Service Provider
CTIA	Wireless Association
DHS	Department of Homeland Security
DoS	Denial of Service
EDGE	Enhanced Data Rates for GSM Evolution
FACH	Forward Access Channel
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIFO	First-In First-Out
FIPS	Federal Information Processing Standard
FirstNet	First Responder Network Authority

GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
IA	Information Assurance
IP	Internet Protocol
IPAWS	Integrated Public Alert and Warning System
IPSec	Internet Protocol Security
ISP	Internet Service Provider
OPEN	Open Platform for Emergency Networks
JHU/APL	The Johns Hopkins University Applied Physics Laboratory
MBMS	Multimedia Broadcast and Multicast Service
MLP	Multi-Level Priority
MPQ	Multi-level Priority Queuing
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
NWS	National Weather Service
PDCH	Packet Data Channel
PDP	Policy Decision Point
PSBN	Public Safety Broadband Network
RF	Radio Frequency
S&T	Science and Technology Directorate
S-CCPCH	Secondary Common Control Physical Channel
TCG	Trusted Computing Group
TCP	Transmission Control Protocol

TLS	Transport Layer Security
TNC	Trusted Network Connect
TS	Technical Specification
UMTS	Universal Mobile Telecommunications System
WEA	Wireless Emergency Alerts
WSDL	Web Services Description Language