Wireless Emergency Alerts: New York City Demonstration

Lessons Learned Report

February 2013

Homeland Security

Science and Technology

Software Engineering Institute
Carnegie Mellon

TASK LEADS
Elizabeth Trocki,
SRA International, Inc.
Jennifer Lavan, SRA International, Inc.
Mark Frankel, New York City Office of Emergency Management
Tamara Marshall-Keim, Software Engineering Institute
Joseph P. Elm, Software Engineering Institute

INSTITUTE STAFF
CERT® Division
Software Solutions Division
SRA International, Inc.

Wireless Emergency Alerts New York City Demonstration

Prepared for
Department of Homeland Security
Science and Technology Directorate, Support to the Homeland Security Enterprise and First Responders Group

ACKNOWLEDGEMENTS

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013 and 252.227-7013 Alternate I.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

Copyright 2013 Carnegie Mellon University

For information about this publication or other SEI research, contact

Software Engineering Institute
Carnegie Mellon University

Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA
Tel (412) 238-5800 • Fax (412) 268-5758 www.sei.cmu.edu

SEI Publication Number: CMU/SEI-2013-SR-tbd

Table of Contents

Executive Summary iii

1 Adopting WEA 1
- NYC OEM 2
- WEA Background 3
- Challenges and Questions 4
- Getting Started 5
- Finding WEA Message Generation Software 7
- Getting Alerting Authority 8
- Putting It All Together 9
- Planning for the Demonstration 10
- Identifying Demonstration Volunteers 11
- Coordinating with Three New Demonstration Partners 12
- Informing the Public 12
- Demonstration Day Approaches 13

2 Lessons Learned 15
- Lesson 1: Coordinating Across Alerting Agencies 15
- Lesson 2: Considerations for Choosing Alert Origination Software 16
- Lesson 3: Building and Maintaining Proficiency 17
- Lesson 4: Factors to Consider Before Sending a WEA Message 18
- Lesson 5: Dealing with the Strengths and Weaknesses of WEA Geo-targeting 20
- Lesson 6: Focusing on Creating Understandable Messages 20
- Lesson 7: Justifying Your Investment in WEA 22
- Lesson 8: Performing Public Outreach 23

3 Conclusion 24

Appendix A Interview with Mark Frankel 25

Appendix B List of Acronyms 37

References and Resources 38

List of Figures

Figure 1: NYC OEM's Communication Pathways Before Adopting WEA 2

Figure 2: Flow of a WEA Message from End to End 4

Figure 3: Four Steps to Sign up for IPAWS [FEMA 2012a] 8

Figure 4: WEA Message Transfer 20

Figure 5: NYC OEM's Communication Pathways Ranked by Severity [adapted from NYC OEM 2012] 32

List of Tables

Table 1: IPAWS-Generated WEA Message Examples 21

Table 2: Mapping CAP Codes to WEA Message Text 21

Table 3: CMAMtext-Generated WEA Message Examples 22

Executive Summary

The Wireless Emergency Alerts (WEA) service, formerly known as the Commercial Mobile Alert Service (CMAS), is a new national capability for delivering geographically-targeted alerts to the public on mobile devices. This report describes the adoption of the WEA service by the New York City Office of Emergency Management (NYC OEM).

NYC OEM was the first alert originator to adopt the WEA service, so the agency experienced some unique challenges. The agency had to obtain software compatible with the Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS), of which WEA is a component, before any vendor had a proven product. NYC OEM also piloted FEMA's four-step process for acquiring emergency alerting authority on IPAWS. In addition, NYC OEM participated in the first regional demonstration of the new WEA service end to end (i.e., successfully originating, authenticating through the Federal alert aggregator, broadcasting, and delivering a WEA message to geographically-targeted mobile devices).

Some of NYC OEM's experiences were specific to being the first alert originator to deploy WEA, but many involved activities that others will have to perform in order to use the WEA service in their own jurisdictions. NYC OEM's information can guide other alert originators in the adoption and integration of the WEA service in the following areas:

- Coordinating alerting authority with local and neighboring jurisdictions
- Choosing alert origination software
- Training staff to send WEA messages
- Determining when to send WEA messages
- Handling the challenges presented by geo-targeting to the county level
- Creating understandable messages in 90 characters
- Justifying investment in WEA
- Informing the public about what to expect from WEA

In the development of this Case Study, the researchers' initial work centered on understanding the operation of WEA. This was accomplished through:

- Review of technical documentation available from FEMA
- Review of technical documentation available from FCC
- Interviews with alert origination service providers (AOSPs) who are developing or have developed products to support WEA
- Interviews with researchers in the field of public alerting

Further work focused on collecting information from NYC OEM that addressed the activities and difficulties they faced in adopting WEA. This data was collected primarily through a series of interviews with NYC OEM staff, including Mark Frankel, the information security officer. This information was interpreted and evaluated in the context of the technical understanding of WEA to:

- Identify challenges faced by NYC OEM that many WEA adopters may experience
- Develop "lessons learned" resulting from the response to these challenges

An appendix includes a sampling of material from these interviews. The questions and answers address organizational learning in the areas of resources, staff buy-in, public outreach, technology, standard operating procedures, and staff training.

1 Adopting WEA

On May 10, 2011, New York City Mayor Michael Bloomberg held a press conference at 2 World Financial Center, overlooking the site of the former World Trade Center. Joining Mayor Bloomberg were Craig Fugate, administrator of the Federal Emergency Management Agency (FEMA), and Julius Genachowski, chairman of the Federal Communications Commission (FCC). The press conference also included high-level representatives from the New York City Police Department, Fire Department, and Office of Emergency Management, as well as the four largest commercial mobile service providers (CMSPs).

Mayor Bloomberg's office called this press conference to announce the launch of a new emergency alert service. The new service, the Wireless Emergency Alerts (WEA), formerly known as the Commercial Mobile Alert Service (CMAS) [1], sends geographically-targeted text messages to any enabled mobile phone in the area of an emergency, and Mayor Bloomberg wanted New York City to have it first. He explained:

> *In both the public and private sectors, I've always believed in the need to harness tech- nology in new ways, including ways that its designers hadn't anticipated. . . . [G]iven the kinds of threats made against New York City at the World Trade Center, Times Square, and other places popular with visitors and tourists, we'll be even safer when authorities can broadcast warnings to everyone in a geographic area regardless of where they came from or bought their phone. I want to congratulate FCC Chairman Julius Genachowski and FEMA Administrator Craig Fugate for this quantum leap forward in using technol- ogy to help keep people safe. [Office of the Mayor 2011b]*

Mayor Bloomberg declared his intention to make this new service available to New York City by the end of the year, a scant seven months away.

Joseph Bruno, commissioner of the New York City Office of Emergency Management (NYC OEM), headed the organization that would be responsible for making this "quantum leap forward" a reality. During the press conference, Commissioner Bruno highlighted two of his primary objectives for implementing WEA: he wanted another tool in the toolbox for notifying the public about emergencies and he wanted to be able to alert a majority of the public, including visitors and tourists, without a subscription requirement. Commissioner Bruno stressed, "If there is an imminent threat to your safety we want to be able to reach you by every means possible, including e-mail, land lines and messages broadcast through [the WEA service]" [Office of the Mayor 2011b]. Commissioner Bruno had committed his organization to deploy WEA on a tight schedule. Now, he had to marshal his resources to meet that commitment.

[1] The WEA service is also referred to as the Personal Localized Alerting Network (PLAN).

NYC OEM

Henry Jackson was in the audience at the press conference that May morning. As the deputy commissioner for technology at NYC OEM, he knew that Mayor Bloomberg would call on his agency to get the WEA service up and running. NYC OEM was chartered in 1996 with the responsibility for communicating alert and notification information to the public during emergency events. New York City has a permanent population of approximately 8 million people as well as thousands of short-term students and approximately 49 million domestic and international visitors annually [Office of the Mayor 2011a; U.S. Census 2012].

Keeping the public informed about emergencies involves many activities. NYC OEM's public warning specialists communicate emergency information to both response agencies and the public before, during, and after an incident. They coordinate emergency response activities among local public safety agencies, including New York City fire, police, and emergency medical services. They also coordinate cross-jurisdictional authorities in neighboring cities and states. In addition to their activities during emergencies, the agency prepares the public for emergencies in advance through education and outreach, by distributing emergency preparation media, and via the agency's website [NYC OEM 2012]. NYC OEM also serves as New York City's primary liaison with the U.S. Department of Homeland Security (DHS) for consequence management and ensures that the city complies with federal preparedness and emergency response requirements.

NYC OEM's public warning specialists already relied on several tools and communication pathways to share emergency information with the public: the Emergency Alert System (EAS), Notify NYC, social media, and traditional media. Figure 1 shows NYC OEM's current tools for alerting the public.

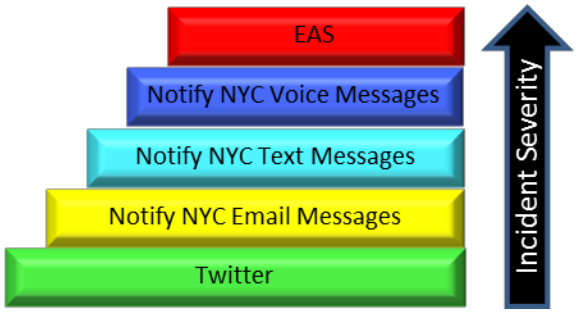

Figure 1: NYC OEM's Communication Pathways Before Adopting WEA

EAS disseminates alerts and warnings to the public via commercial television and radio and can potentially broadcast across the entire New York City metropolitan area. NYC OEM has the authority to send messages over EAS for non-weather emergencies. While the National Weather Service (NWS) routinely issues weather-related EAS messages in New York City, NYC OEM reserves EAS for only the most severe emergency incidents and has never direct-

ly issued a local EAS message to the public.[2] EAS is one communication channel provided by FEMA's Integrated Public Alert and Warning System (IPAWS). IPAWS is a nationwide system that enables local, tribal, state, territorial, and federal authorities to submit alerts for dissemination to the public via television stations, radio stations, weather radio, internet, and other communication channels. WEA is one of the IPAWS channels and distributes alerts to mobile phones.

Notify NYC is NYC OEM's primary channel to communicate emergency information to the public. Notify NYC is a free, subscription-based service that distributes information about emergency incidents and city services (e.g., subway and utility disruptions, parking rule suspensions, and public school closures) via e-mail, short message service (SMS) text messages, and voice messages to landline and mobile phones. However, its subscriber base of 100,000 people reaches only a small fraction of the city's 8 million residents and 49 million annual visitors.

The Notify NYC service also includes social media communications. NYC OEM's public warning specialists distribute information about emergency incidents and city services via Twitter, Really Simple Syndication (RSS) feed, and the agency's Facebook page. The RSS feed averages 120,000 views per month, and the Twitter feed has approximately 38,000 followers. However, the agency does not rely heavily on social media to monitor or manage public response to emergencies. Mayor Bloomberg and Commissioner Bruno were counting on WEA to significantly enhance the city's ability to get information directly to all members of the public near an emergency incident without relying on a limited base of subscribers, followers, and website visitors.

NYC OEM has a strong relationship with the media and maintains a staff of press liaisons to work closely with them during emergencies. During large-scale incidents, the agency often establishes a joint information center on-site to help the media get emergency information to the public. Although the public warning specialists value their ability to share information with the public via the media during emergency incidents, they always first use the agency's own tools before using the media to share identical or supplementary information.

WEA Background

The WEA service enables local, tribal, state, territorial, and federal public safety officials to send geographically-targeted text alerts to the

WEA Message Types

Presidential Alerts: Alerts issued by the president of the United States to all citizens

Imminent Threat Alerts: Alerts involving serious threats to life and property, often related to severe weather

AMBER Alerts: Alerts regarding missing or abducted children

[2] NYC OEM attempted to issue an EAS message on September 11, 2001. However, the infrastructure failed to disseminate it. The infrastructure failure has been addressed since 2001.

public.The DHS Science and Technology Directorate (S&T) partners with FEMA, the FCC, and CMSPs to enhance public safety through the deployment of WEA. WEA is one of the major components of IPAWS, and it uses FEMA's IPAWS Open Platform for Emergency Networks (IPAWS-OPEN) to permit emergency management agencies nationwide to submit alerts for public distribution [FEMA 2012b]. The WEA service can send three types of messages. The President of the United States can issue a Presidential Alert to reach any region of the nation, or the nation as a whole. Emergency management agencies can issue Imminent Threat Alerts and AMBER (America's Missing: Broadcast Emergency Response) Alerts.

CMSPs relay these alerts from IPAWS-OPEN to mobile phones using cell broadcast technology, which does not get backlogged during times of emergency when wireless voice and data services are highly congested (see Figure 2). Customers of participating CMSPs who own WEA-capable mobile phones will automatically receive these alerts during an emergency if they are located in or travel to the affected geographic area.[3] At this time, the WEA specification required alerts to be geo-targeted to the county level at a minimum. They can contain no more than 90 characters of text, no hyperlinks, no pictures, and no other nontext data.

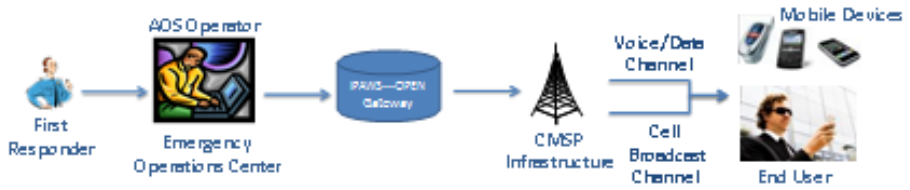

Figure 2: Flow of a WEA Message from End to End

Challenges and Questions

At the time of Mayor Bloomberg's announcement, no emergency management agency had deployed WEA; NYC OEM would be the first. Jackson had no examples to follow. From the outset, he faced daunting challenges, the biggest being the seven-month timeline dictated by Mayor Bloomberg's announcement.

The other big challenge was the readiness of the WEA service. The service was not scheduled to deploy until April 2012. FEMA was still conducting internal testing; upgrading to IPAWS-OPEN; and establishing each of the system gateways between originators, IPAWS-OPEN, and the CMSPs. The major CMSPs had also been working toward the national April 2012 deadline. Would the WEA service be ready for Jackson by December 2011? Was it stable enough now to enable him to start his efforts toward deployment?

Jackson also knew he would need software to create the WEA messages and relay them to IPAWS-OPEN. Could he find a supplier of this software, or would he have to develop it himself?

[3] The *Code of Federal Regulations* publishes rules for WEA, and the FCC maintains a list of CMSPs currently participating in WEA [CFR 2012; FCC 2012b].

Jackson did have prior experience that would be useful in this project. He was familiar with IPAWS and standards-based information sharing, such as the Emergency Data Exchange Language (EDXL) and the Common Alerting Protocol (CAP), a standards-based language used in IPAWS. Jackson also had established relationships with the FEMA IPAWS Program Office, the Organization for the Advancement of Structured Information Standards (OASIS), and New York State emergency management authorities.

Jackson had a basic understanding of the WEA service. He knew that WEA was one of several dissemination channels within IPAWS and a capability that would enable the agency to issue alerts to all owners of WEA-capable mobile phones, including the city's permanent residents as well as visitors located within a specific geo-targeted area when the alert is sent. But he also had some questions about WEA.

The WEA specification requires CMSPs to geo-target messages at the county level. However, Jackson had heard from some CMSPs that the WEA service could geo-target alerts to a single city block. Would all CMSPs provide this capability, or would some geo-target only to the county level per the minimum requirement of the WEA specification? Without consistency across the CMSPs, he couldn't count on the finer resolution geo-targeting.

Jackson was also concerned about developing understandable WEA messages. WEA messages are originated by communicating with IPAWS-OPEN in a message conforming to the CAP format. A CAP message contains a number of fields that define the characteristics of an emergency, including location, severity, effective date and time, event description, and instructions. In many cases, WEA messages are automatically constructed from the contents of these fields, producing messages that can be somewhat cryptic. It was possible to override this automatic message construction and directly enter a message of 90 characters or less. But use of this method required special permission from FEMA. And even if he obtained permission, crafting 90-character messages conveying both the nature of the emergency and recommended actions for the public would be difficult.

Getting Started

Immediately after the press conference, Jackson began enlisting aid from people within NYC OEM as well as other agencies. His first calls went to the FCC and FEMA. These agencies had collaborated to bring WEA into existence. The FCC had worked with the CMSPs to obtain their participation and to develop the rules and orders for WEA [FCC 2008, 2012a]. FEMA had designed IPAWS and the architecture to gather and distribute the alert messages. Jackson discussed his plans to have WEA up and running in New York City before the end of the year. In short order, all agreed that they would need some form of test or demonstration to support this goal.

DHS S&T would also participate in this plan to demonstrate the performance of WEA. S&T had recently received funding from the National Telecommunications and Information Administration to test WEA at both the national and regional levels and wanted to include alert originators, FEMA, and CMSPs in its first demonstration event. Together, these players col-

laborated and envisioned an end-to-end demonstration in which NYC OEM would create and send demonstration WEA messages. FEMA's IPAWS-OPEN would vet the alerts and relay them to the CMSPs' interfaces, and the major CMSPs would transmit the demonstration alerts to mobile phones in geo-targeted areas of New York City.

Jackson believed that a demonstration of this nature was essential to his goal of deploying in December. It would focus all of the parties on overcoming the many obstacles that lay between them and their goal. It would enable NYC OEM to perform due diligence on the WEA service, demonstrating that it could, in fact, disseminate alerts reliably to WEA-capable mobile phones in New York City. Finally, it would enable the agency to see the WEA service at work and assess its ability to geo-target alerts and the ability of WEA-capable mobile phones to display them. These were unknowns, and Jackson believed that the demonstration results would inform the agency's technical, standard operating procedures (SOPs), and training activities.

S&T and FEMA expected that they could be ready to demonstrate WEA several weeks before Jackson's December 2011 deployment deadline. As planning began, S&T, FEMA, NYC OEM, and one CMSP had agreed to participate in the demonstration.

Jackson then turned his attention to getting NYC OEM ready for its role in the demonstration. He saw WEA as an extension of the Notify NYC service, augmenting, but not replacing, the other tools and services in use by the agency. He planned an adoption process that reflected this approach through five steps:

1. Plan and staff the adoption project.
2. Obtain IPAWS-compatible software through an alert origination service provider (AOSP).
3. Obtain IPAWS alerting authority from FEMA.
4. Demonstrate the system to confirm that it is working in New York City and to better understand its capabilities.
5. Use the demonstration outcomes to develop SOPs and training materials for NYC OEM's WEA message originators.

His first step was to line up the resources needed to adopt and deploy WEA. Jackson's Technology Division in NYC OEM would do most of the work to adopt the WEA service. But Jackson would have to engage several other divisions within the agency to help with activities outside the scope of technology integration.

He would need the assistance of the Operations Division, which is the home of the public warning specialists who monitor emergency activity and originate alerts and warnings to the public. Initially, Jackson asked them to provide advice on the human interface needed for WEA. Later, they would participate in demonstration activities, help develop SOPs, and take over operational responsibilities once adoption and demonstration activities were complete.

He would need the assistance of the Legal Affairs Division to review all the agreements that NYC OEM had to complete as part of its WEA adoption process, including memorandums of

agreement (MOA) with FEMA. He would need some help from the External Affairs Division, which coordinates the agency's volunteers for training exercises and surge support during emergency events. He anticipated that volunteers would carry mobile phones during the demonstration event. He also planned to use the division to assist with distributing information to the public and other New York City agencies. Finally, he anticipated a need for the Strategic Data Division to provide reliable geospatial data for demonstrating the WEA service's geo-targeting capabilities locally.

Finding WEA Message Generation Software

With his staffing and resources planning settled, Jackson turned his attention to obtaining IPAWS-compatible software to originate WEA messages. Jackson's information security officer, Mark Frankel, had been assisting in many of the WEA efforts. Jackson now turned to him to solve the message origination problem.

Frankel first approached the AOSP that was currently supporting NYC OEM's software needs to explore the availability of WEA message origination software. It had none. In fact, its current products were not CAP based or IPAWS compliant, so the AOSP would need to invest in a significant development effort before NYC OEM could use their product to issue WEA messages.

Frankel began a campaign to identify alternative AOSPs that could provide the software that he needed. Many AOSPs were just starting to develop products that were truly capable of issuing WEA messages. And FEMA was still defining the processes for becoming an approved vendor of IPAWS-compatible software. No one had a product proven and ready to go.

At this time, attention to the upcoming demonstration was beginning to grow. The MITRE Corporation, a not-for-profit organization chartered to provide systems engineering expertise and acquisition strategy advice to sponsors like DHS, of which S&T and FEMA are components, had also heard about the demonstration partners' planning activities. MITRE was aware of a Canadian open-source, CAP-based tool and volunteered to adapt it to meet the needs of NYC OEM for the demonstration event. MITRE believed it could deliver within the deadline. Frankel was convinced that MITRE could adapt its tool to meet NYC OEM's needs and IPAWS's requirements more quickly than he could obtain other IPAWS-compliant software to originate alerts.

NYC OEM's existing AOSP had also heard about the upcoming demonstration event. While the AOSP did not have software compatible with IPAWS-OPEN, it did have software compatible with Disaster Management-OPEN, the predecessor to IPAWS-OPEN. The AOSP realized that future business relied on being compatible with IPAWS-OPEN, so it also volunteered to develop software to support NYC OEM's upcoming demonstration. While Frankel was concerned about the AOSP's ability to meet the deadline for the demonstration, he accepted this offer because it provided a back-up plan to MITRE's software adaption activities and increased the likelihood that the agency would be ready for the demonstration.

Now Frankel had two software suppliers, each developing prototype products to support the demonstration. Frankel worked closely with each supplier to make sure that its solution's capabilities and user interface would meet the agency's needs. As they developed the products, the AOSPs provided frequent demonstrations to NYC OEM and collected suggestions for upgrades and revisions. The two suppliers were taking different approaches. MITRE's solution was operated and maintained remotely by MITRE and accessed by NYC OEM via a web interface. The tool developed by NYC OEM's existing AOSP would be installed on NYC OEM's hardware and maintained similarly to its Notify NYC tool, for which the agency had maintenance and data-recovery plans [NYC DOITT 2012]. Each supplier also had to execute an MOA with FEMA to gain access to the IPAWS-OPEN testing and development environment, in which it would test its solution and confirm that its software was compatible with IPAWS before NYC OEM began using it.

Getting Alerting Authority

Jackson turned his attention to obtaining IPAWS alerting authority from FEMA. Signing up for access to IPAWS is a four-step process, shown in Figure 3. The first step, obtaining IPAWS-compatible software, was underway.

Figure 3: Four Steps to Sign up for IPAWS [FEMA 2012a]

The second step in the process is to sign an MOA with FEMA. To address concerns of system security, the MOA requires a list of all systems that will interoperate with WEA [FEMA 2012e]. While completing the MOA was relatively straightforward, NYC OEM had a large number of software products and tools, and Jackson was unsure which should be included on the MOA. He also did not know whether he would need to submit a separate MOA for each product and tool. Jackson worked with his contacts in the FEMA IPAWS Program Office to verify that NYC OEM needed to submit just one MOA and include only the systems that NYC OEM planned to use to interoperate with WEA.

Next, Jackson needed to determine the scope of NYC OEM's alerting authority. He communicated with other agencies to select the specific alerting permissions for which his agency would apply. NYC OEM is the only local authority within New York City that can send non-weather Imminent Threat Alerts. The agency cannot issue Presidential Alerts and does not issue AMBER Alerts. Alerts for missing persons are routed to the state-level Missing Persons Clearinghouse in Albany, New York, which issues AMBER Alerts to the relevant local juris-

diction. Jackson also contacted NWS to discuss the alerting responsibilities for imminent threats that result from fast-moving weather conditions. Since NWS was not currently using WEA for weather-related alerts, Jackson told them that NYC OEM planned to retain the authority to originate alerts for weather events such as tornadoes, flash floods, and severe thunderstorms. They could revisit this decision later if and when NWS adopted WEA.[4]

> Based on these discussions of NYC OEM's alerting authorities, Jackson started the process of applying to FEMA for public alerting permissions. He cited NYC OEM's intent to issue Im-- minent Threat Alerts only, including alerts for non--weather and weather--related events. Be-- fore submitting the application to FEMA, he needed approval from New York State. NYC OEM's leadership had to do some research and networking to identify the appropriate state agency to contact. Jackson submitted the application to state authorities to obtain permission for alerting. Once he received state approval, Frankel submitted the completed and signed application to FEMA. After approval, FEMA responded by assigning NYC OEM an IPAWS Collaborative Operating Group (COG) ID and digital certificate. The COG ID is a name and number used by IPAWS to designate an organization that is responsible for coordinating emergency management activities. The digital certificate "signs" every alert message that an organization sends to IPAWS and ensures the identity of the originating COG. With the COG ID and digital certificate, NYC OEM could access IPAWS--OPEN.

One final step in acquiring alerting authority was to satisfy FEMA's training requirement. FEMA had drafted an online training course for independent study called IS-247: Integrated Public Alert and Warning System (IPAWS) [FEMA 2012d]. The course provides basic information about IPAWS and guidance for composing messages in CAP and crafting effective message content to alert and warn the public. Members of the Technology Division and public warning specialists who were scheduled to participate in the demonstration took the draft IS-247 training course and provided FEMA with feedback on the instruction.

Putting It All Together

Both software products progressed toward completion. FEMA had provided the COG ID and digital certificate needed to access IPAWS-OPEN when the agency completed the alerting authority process. Once Jackson and Frankel were satisfied with the software solution from each supplier, Frankel configured the COG ID and certificate with each software product and established its COG member permissions. Frankel continued to conduct meetings with the AOSPs to ensure that each met the prerequisites before the demonstration. They each needed to sign FEMA's developer MOA and Rules of Behavior; establish Internet Protocol Security; test the IPAWS-OPEN A-Interface, which is the primary interface between alert originators and IPAWS-OPEN; and confirm beta test system readiness.

---

[4] Later, in summer 2012, after both NYC OEM and NWS had fully adopted WEA, NYC OEM and New York City's local NWS office determined that NWS would serve as the primary alert originator for WEA weather alerts in New York City. NYC OEM serves as a backup alert originator for fast-moving weather events and will issue a WEA weather alert only if NWS requests or acknowledges that NYC OEM take this action.

The suppliers tested their software in FEMA's testing and development environment to certify it as IPAWS compatible. Frankel and the AOSPs also tested the software internally to determine that it was operating properly on NYC OEM's servers, and they issued multiple test messages to the IPAWS-OPEN testing and development environment to confirm that NYC OEM's system was communicating properly with IPAWS-OPEN and receiving acknowledgment messages from IPAWS. Frankel did not issue any live test alerts to the IPAWS-OPEN production environment before the official demonstration because he was concerned that live test alerts would reach the public's WEA-capable mobile phones before the agency's press officers had notified the public about the WEA demonstration.

Planning for the Demonstration

Frankel oversaw the agency's participation in the demonstration and coordinated internally with Jackson, other NYC OEM divisions, and city officials as needed. S&T owned the demonstration event and coordinated the other partners' activities throughout the process. As planning kicked off, Frankel and Jackson participated in weekly calls with the demonstration partners to develop the plan and procedures. Revisions to the procedures took place iteratively throughout the planning effort. Over time, the partners shaped the plan to verify the processes of originating a CAP message at NYC OEM, authenticating the message through IPAWS-OPEN, delivering the message to the CMSP gateways, and ultimately disseminating the message to mobile phones located in New York City. Per the resulting procedures, WEA messages would be delivered directly to the public during the demonstration. Given the risks involved in issuing demonstration messages to New York City's public, Frankel worked closely with Jackson, Commissioner Bruno, and the Mayor's Office on decisions and actions related to informing the public about the demonstration and clearly marking the messages as for demonstration purposes only. Leadership approved the wording of the messages. The procedures also identified NYC OEM as the alert originator, with the agency's headquarters serving as the demonstration's operations center.

As a result, NYC OEM gradually transitioned into a demonstration-host role as the event date approached, with Frankel as the lead. Two of the host's key responsibilities were to serve as the primary point of contact for all demonstration partners and to serve as the geographic location expert and authority, specifically to determine the locations that would be geo-targeted for WEA messages during the demonstration.

In fulfilling this role, Frankel worked with his Operations Division and S&T to develop test cases for use during the demonstration. Each test case identified the purpose of the case, the requirement it addressed, the message type, each partner's role in completing the case, prerequisites, and steps to complete the case procedure. Together, NYC OEM and S&T also developed the sequence and timing of the test cases and vetted the details with all the CMSPs.

The CMSP partner conducted tower testing in New York City before the demonstration and met with Frankel several times during the planning to improve NYC OEM's understanding of the CMSP's pre-demonstration activities. The CMSP needed to ensure that cell towers were working correctly in the city, meet the anticipated level and granularity of coverage in the

city, and decide which types of mobile phones that it would make available for the demonstration.

To fulfill the second role as the demonstration partners' geographic location expert, Frankel engaged NYC OEM's Strategic Data Division. This division is responsible for providing geospatial data for emergency planning purposes. The procedures developed by the partners resolved that alerts would be geo-targeted at and below the county level during the demonstration. While the WEA specification requires CMSPs to be able to disseminate WEA messages only at the county level, the CMSP partner was able to geo-target below the county level, and all partners believed it was valuable to gather data points regarding this finer resolution of geo-targeting, too. Frankel worked with the Strategic Data Division to identify the best areas to geo-target the demonstration alerts to gather information about the accuracy of WEA geo-targeting at and below the county level, as well as the degree of WEA message bleed-over to areas outside the target area. *Bleed-over*-when messages broadcast to a defined area are received by mobile phones outside of that area-is more likely to occur in areas with cell towers that span more than one county or cover large areas. In urban areas, where several cell towers are located in close proximity, CMSPs have a better ability to control coverage with finer granularity, reducing bleed-over.

Frankel and the Operations Division decided that the agency would issue one demonstration message to all five counties in New York City and one demonstration message to each individual county to confirm that WEA geo-targeting at the county level was operating properly. They also identified two areas of the city that were both congested and near county borders to test for potential bleed-over across New York City's internal county lines as well as bleed-over into neighboring jurisdictions in New York State and New Jersey. The Strategic Data Division then helped map these areas so they could be plotted correctly using the polygon capability of each IPAWS-compatible software product. The data sets resulting from the demonstration would help the CMSPs ensure that the system was working properly in New York City, determine that the CMSP's towers were communicating with IPAWS-OPEN appropriately, and inform the development of NYC OEM's SOPs for the WEA service.

Identifying Demonstration Volunteers

Frankel needed to provide volunteers to carry mobile phones during the event. The partner CMSP would deliver 30 mobile phones for the demonstration. Frankel worked with NYC OEM's External Affairs Division, which has a dedicated staff of volunteer coordinators. These volunteer coordinators could assemble the volunteers who would carry mobile phones in the field throughout the demonstration. The volunteers would fan out inside and outside the geo-targeted area so that their mobile phones could collect data regarding message delivery and bleed-over in various geographic areas of New York City, including in-building, subway, waterfront, and borough-border locations.

The volunteer coordinators contacted their standing pool of volunteers to assess their availability and suitability for the demonstration, specifically looking to recruit tech-savvy volunteers who could learn to operate new-to-market WEA-capable devices on the morning of the

demonstration. The volunteer coordinators also determined the type of information and level of detail that volunteers should receive about the demonstration and their participation in it, and they developed information packets based on this determination. Closer to demonstration day, the volunteer coordinators would also plan for training the selected volunteers.

Coordinating with Three New Demonstration Partners

A few weeks before demonstration day, the other three major CMSPs accepted S&T's long-standing offer to participate in the December 2011 demonstration. The original CMSP partner had completed all the necessary prerequisites, was ready to demonstrate at this point, and had made several trips to New York City to ensure that its network's cell broadcast technology and its interface to IPAWS-OPEN were functioning properly. Adding three more CMSPs to the demonstration partnership introduced a new dynamic to the final planning activities and delayed the demonstration date several times. Now, each additional CMSP needed to complete the following prerequisites to participate in the demonstration:

- Sign the FEMA MOA and the Interconnection Security Agreement.
- Confirm availability of resources to perform connection and testing.
- Establish Internet Protocol Security with IPAWS-OPEN.
- Perform interface tests mandated by FEMA for IPAWS-OPEN.
- Confirm operational readiness to perform their part of the end-to-end demonstration.

Introducing three new CMSPs also increased the number and length of planning calls with all of the demonstration partners. These calls focused on determining the status of each CMSP's completion of prerequisites and the resulting delays to the demonstration date. Several demonstration partners experienced technical issues with their connections to IPAWS-OPEN and communication with CMSP cell towers, requiring postponements.

In addition to causing delays, each new CMSP also provided their own mobile phones for the demonstration event. This increased the required number of volunteers to approximately 100, thereby increasing the level of coordination with volunteers. The volunteer coordinators' strong relationship with the agency's standing pool of volunteers was extremely valuable in recruiting new mobile phone carriers for the demonstration, especially as the partners had to delay the event several times during the November-December holiday season. The volunteer coordinators needed to vet proposed dates with the volunteers twice to confirm their availability and request their commitment to participate in the demonstration on the scheduled date.

Informing the Public

NYC OEM anticipated that members of the public in New York City would receive demonstration messages if they owned WEA-capable mobile phones. Frankel needed to prepare the public. Frankel had been engaging NYC OEM's deputy commissioner for external affairs for several weeks leading up to the demonstration to define the need for outreach to the public. Together they decided to draft a press release and disseminate it to the local media [NYC

OEM 2011]. Frankel worked with Jackson, the Mayor's Office, and NYC OEM's press officers to issue the press release before the demonstration. Frankel also coordinated with the other demonstration partners to ensure that everyone agreed to the content. The press release provided an overview of what the WEA service is, how an alert might display on mobile phones, and the date and partners participating in the demonstration. It also let the public know that they might receive demonstration messages during the event. In response to the press release, the local media advertised the event on radio and television programs immediately prior to the demonstration.

To inform other emergency management agencies about the new WEA service, the Operations Division wrote and vetted a communication with the NYC OEM staff engaged in planning for the demonstration. They then sent this as an e-mail to the city's 911 and 311 call centers to notify them in advance of the December 2011 WEA demonstration event. These centers routinely receive calls from the public when people are unsure how to respond to an alert message or emergency event, and the Operations Division wanted them to be prepared. They also sent the same e-mail to other key agencies in New York City (e.g., New York City Police Department, New York City Fire Department, and New York City Hall) and parallel agencies in neighboring jurisdictions in New York and New Jersey to notify them of demonstration activity. Possibly, WEA messages would broadcast to cell towers in adjacent areas not intended to receive the demonstration messages, and NYC OEM wanted neighboring jurisdictions to be prepared as well. As a result of their outreach to the public, the city's 911 and 311 call centers reported no calls or concerns from the public about receiving WEA messages during or after the demonstration.

A few days before the demonstration in New York City, without the knowledge or participation of NYC OEM or FEMA, a CMSP in New Jersey accidentally disseminated a test message to the public via the WEA service. The content of the message did not include the word "test" and startled members of the public as well as local emergency management officials, who were unaware of any WEA testing. While the test message was unrelated to preparations in New York City, it garnered a fair amount of attention by the media and was precisely the type of negative publicity that NYC OEM hoped to avoid in conducting its own demonstration of WEA. The actions that NYC OEM took to inform the public in advance of the demonstration in New York City helped ensure that it did not catch the public by surprise.

Demonstration Day Approaches

Frankel received the mobile phones from CMSPs within days of the demonstration and worked with their sales executives and engineers to determine that the mobile phones were working and questions about using them had been addressed.

Leading up to demonstration day, Frankel, the volunteer coordinators, and the Operations Division conducted exercises internally, role playing scenarios of the actions that NYC OEM would ask volunteers to perform. They brainstormed how volunteers might interpret and complete the requested actions and considered potential questions they might pose. These exercises helped them identify gaps in the scenarios, and they revised their guidance for the volunteers accordingly. This activity helped the agency ensure that volunteers' actions mirrored the intent of NYC OEM's guidance.

The volunteer coordinators worked with S&T and Frankel to develop instructions for volunteers, informing them of the location for each demonstration message, the message content they should see, and the time they should see each message. To help measure results, the volunteers who carried the mobile phones would complete observation forms. These forms documented information about the time and location of volunteers when their mobile phones received demonstration messages, details about their surroundings at that time, and information about how messages displayed on the mobile phones.

The night before the demonstration, Frankel led a kick-off meeting. During this meeting, the volunteer coordinators relayed detailed instructions about how the volunteers should use the mobile phones, the data collection templates, and what to do during the demonstration.

When demonstration day finally arrived, Jackson, Frankel, and their partners were ready: The necessary MOAs with FEMA were approved. Software from both the current AOSP and from MITRE was installed and configured with the appropriate FEMA certificates. Initial testing showed that they were both operational. A few members of Jackson's staff were trained to use them. IPAWS-OPEN was up and running, and initial tests had confirmed communication with the message generation software. Communication within the WEA service seemed to be working. Through their own internal testing, the CMSPs were confident that they could receive and transmit the WEA messages. Volunteers had been recruited to take positions within New York City with various makes and models of mobile phones connected to the four participating CMSPs. And demonstration plans and procedures were in place. It was time to run the demonstration.

2 Lessons Learned

In developing the information provided in this chapter, the authors drew primarily on the experiences of the research team of the Carnegie Mellon Software Engineering Institute, the staff of SRA International, Inc., and the staff of NYC OEM during the preparation and performance of the WEA demonstration in New York City. During this time, these contributors made numerous observations regarding both the operational characteristics of the WEA service and the adoption processes utilized by NYC OEM. These observations exposed particular challenges that many emergency management agencies (EMAs) could be expected to face when adopting CMAS. Subsequent to the demonstration, the research team continued to explore these challenges through

- Review of academic literature in the field of public alerting [Mileti 1991] [Mileti 2000]
- Discussions with other EMAs
- Discussions with suppliers of support software for the WEA service
- Other researchers in the field of public alerting

The resulting lessons presented in this chapter represent the findings of this research.

Lesson 1: Coordinating Across Alerting Agencies

Overlapping jurisdictions-such as nations, states within the nation, counties within a state, and municipalities within a county-are common and complicate the process of public alerting. Even within a single jurisdiction, multiple agencies such as the police department and fire department may have authority to issue public alerts.

Effective alerting demands the presentation of clear and unambiguous information to the public. When multiple agencies possess the ability to issue alerts in an area, confusion can arise from redundant or contradictory alerts. Avoiding this situation demands coordination across all involved EMAs.

When applying for public alerting permissions, EMAs should coordinate with other alerting agencies to determine the scope of their alerting authorities and to define their roles in anticipated emergency situations. For example, alerting for all weather-related emergencies may be reserved for the local NWS office, and AMBER alerting may be reserved for a designated state emergency management agency. Consider cases where an emergency event may cross jurisdictional boundaries, such as a drifting cloud of toxic gases released from an industrial accident, or a flood resulting from a dam break. Establish agreements with adjacent jurisdictions that address coordination of alerting to avoid inconsistencies and redundancies. After WEA deployment, continue coordination with these other agencies to ensure timely and accurate alerting.

Lesson 2: Considerations for Choosing Alert Origination Software

EMAs should consider a number of factors when choosing an alert origination software product or service.

1. EMAs must choose a product that meets the technical needs of the WEA service;; it must be CAP compliant and IPAWS--OPEN compatible.
2. EMAs must make some decisions about how the organization intends to use WEA service.
    - Specify the kinds of alerts that the EMA will issue: Imminent Threat Alerts or AMBER Alerts.
    - Decide whether to construct WEA messages using Commercial Mobile Alert Message text (CMAMtext), or to let IPAWS-OPEN assemble WEA messages from the required CAP fields. If you elect to use CMAMtext, apply to your state alerting authority and FEMA to obtain permission.
    - Decide whether to draft each message individually or to use standardized templates. Communicating these decisions to the AOSP is important to ensure that the provider delivers a satisfactory system.
3. Address questions of integration with your other systems. Some factors to consider in deciding to choose an integrated or a stand--alone system include acquisition cost, user workload, training costs, and maintenance costs.
    - A stand-alone system may be easier to acquire; however, it could increase staff workload, forcing redundant actions to issue an alert over multiple channels, including WEA. A separate system may also increase training and maintenance costs.
    - An integrated system can enable creation of one message and dissemination to all appropriate channels. It can reduce workload by eliminating the need to monitor multiple systems. Lower initial and ongoing training costs may result if the user interfaces are similar to those already in use. Maintenance costs may also be lower.

    However, choosing a system integrated with other alerting capabilities may restrict procurement options to working solely with the current AOSP.
4. Security is a key factor to consider. The COG digital certificate issued by FEMA controls access to IPAWS--OPEN. But the responsibility for controlling internal access to alerting systems lies with the EMA. In addition to basic security measures (e.g., firewalls, anti--virus tools, anti--spyware tools) maintained by the EMA IT department or service, ensure that the acquired alerting software has strong access controls requiring authentication of users. Policies should require strong passwords that are updated frequently.
5. Software acquisition results not only in purchasing software but also in committing to the concept of operations embedded in that software. Purchased alert software should suit the operational concepts of the EMA. Failure to plan for this will result in a continual struggle to make the software support EMA operations effectively. The user interface is also a major discriminating factor among the potential suppliers. Choose one that supports the

current EMA operations.

6. System support is a crucial factor to consider when choosing alerting software.
    - For an alerting solution hosted internally, the EMA must have the ability to support and update it. In addition to the initial purchase cost, annual license and maintenance fees may also be required.
    - For an alerting solution hosted externally (e.g., a web-based service), the solution provider will take care of support and updates. EMA operating costs will include an- nual or monthly subscription fees. Ensure that the provider will supply the required level of service. A key question to address is access to the service through jammed or damaged communication channels during a real emergency.
    - Consider factors affecting continuity of operations, such as support of remote employees, mobile alerting capabilities, and contingent operations in disruptive circums- tances.

Lesson 3: Building and Maintaining Proficiency

Proficiency with WEA tools and operations is critical for effective crisis management. Before deploying WEA, EMA staff must have the skills to use it effectively. This requires training. Start with FEMA's IS-247 training course, which offers a good overview of IPAWS, instruction on how to compose messages in CAP, and guidance on writing an effective message. Although FEMA requires only one representative from each COG to participate in the training, it is beneficial to have all personnel who are authorized to issue WEA messages complete the training. In addition to the FEMA training, also consider:

- Specific training and materials that cover EMA SOPs. Create training that clearly identi- fies the criteria for issuing a WEA message and the authorizations required to do so.
- Training specific to the alert generation software. If an AOSP supplied the software, con- sult them for user training. Consider developing a short how-to manual illustrated with screenshots.

Maintaining WEA proficiency is a continuing challenge. Remember that training is not a one-time event. Over the years, as personnel are added or replaced, the new staff will require training. Make sure that courses and materials remain current to support ongoing training.

Because WEA messages are intended for severe and extreme emergencies, EMA staff will not issue them frequently. However, when EMA staff need to issue a WEA message, they must to do so quickly. They will not have time to re-familiarize themselves with alert generation processes or systems. It is important to have a program in place that maintains proficiency. There are several ways to maintain this proficiency:

- *Periodic training:* Establish a training program that provides both initial and periodic refresher training for all alert originators. This training should address both the policies and procedures for issuing WEA messages as well as using the alerting software to gen- erate the alerts.

The process of creating an understandable 90-character WEA message is a particularly

important function to train and practice.

- If EMA processes call for alert creation by letting IPAWS-OPEN assemble WEA messages using data from CAP fields, staff must understand how IPAWS-OPEN assembles the message so that they can supply CAP fields with appropriate data to create an understandable message.
- If EMA processes call for alert construction with CMAMtext,[5] staff must be able to quickly craft a 90-character message that is easily understood.
- In both cases, templates can be useful in ensuring that the message includes critical information and satisfies constraints (e.g., the 90-character limit).

EMAs should perform training frequently enough to ensure the necessary proficiency. To determine training frequency, EMAs should periodically test the proficiency of the alert generation staff. If they do not meet performance standards, they may need more frequent or more detailed training.

- *Routine drilling:* Although EMA staff will not issue WEA messages for every emergency, they can use a subset of such emergencies for practicing alert generation. Define a practice frequency, such as one per week or one per month, to practice creating and processing WEA messages. As the EMA addresses emergencies on a day-to-day basis, exercise the policies and procedures for generating a WEA message.

  Practicing operation of the alert generation software is also desirable; however, practicing on a "live" system contains some risk of inadvertently issuing an unwarranted alert to the public. FEMA maintains the Joint Interoperability Test Command (JITC) test environment in which EMAs can test and verify their alerting capabilities. This environment emulates the IPAWS-OPEN and WEA services. EMAs can send CAP-compliant messages to this environment to verify message acceptability. This enables the alert originator to practice alert system operation in a low-risk environment.

Lesson 4: Factors to Consider Before Sending a WEA Message

WEA enhances public safety by capitalizing on the increased use of mobile devices in the United States today. It provides for the distribution of alerts and warnings to the public based on their current location. This enables alerters to reach not only residents in a threatened area but also people who work in that area as well as visitors just passing through. The WEA service is intended to distribute alerts only in severe and extreme emergencies to raise the public's awareness about an emergency incident and direct them to take specific action/seek more information to avoid harm. The types of emergencies for which EMAs should consider using WEA include:

- An emergency incident expected to cause other emergencies
- An emergency incident with a wide geographic impact and severe or extreme results
- An emergency incident with a limited geographic impact and severe or extreme results
- An emergency incident that may overburden the 911 system as a result of the public' s increased level of concern, need to report information, or need to gather

information

[5] Using CMAMtext requires approval from FEMA.

- An emergency incident that requires all or a portion of the public to evacuate, take shel- ter, or take other preventive action

An EMA should establish policies and procedures that clearly define the circumstances and criteria for issuing a WEA message. Waiting until an actual emergency to determine these factors will delay the public's receipt of an alert and decrease its value. Policies should be informed by both FEMA recommendations and WEA capabilities. Factors to consider include

- *Severity and urgency:* EMAs should use WEA to issue alerts only in extreme or severe emergencies, when immediate action is needed. Policies should clearly define what types of emergencies are sufficiently severe to warrant a WEA message.
- *County-level geo-targeting:* Minimum WEA geo-targeting resolution is at the county lev- el. EMAs should expect WEA messages to be broadcast to everyone in the specified county, as well as to some in neighboring counties, as the alert "bleeds over" into nearby areas. Issuing a WEA message that is relevant only to a small geographic area (e.g., a township or a few city blocks) will result in many people receiving an alert that is not re- levant to them. If using CMAMtext to generate the WEA message, EMA staff can include information further delineating the affected area (e.g., "affects zip code 12345" or "af- fects Grant Township"); however, the message may still be received beyond the specified area.

Policies should address a balance between the public safety value of alerting versus the impact of over-alerting (see "alert fatigue" below). EMAs should issue WEA messages only when the benefit of reaching members of the public in need of urgent information outweighs the detriment of alerting members of the public not affected by the event.

- *Degree of certainty:* The WEA service is reserved for alerts that rise to an *observed* or *likely* certainty. During an emergency, information can be absent, delayed, and contradic- tory. As more information is gathered, a clearer understanding of the situation emerges and the degree of certainty regarding the event increases. EMA policies should clearly identify what level of certainty is needed (e.g., confirmation from *x* independent sources, eyes on the scene) before issuing a WEA message.
- *Alert fatigue:* Alert fatigue occurs when the public receives WEA messages too frequent- ly. Alert fatigue applies primarily to alerts that are not relevant to the recipient. Most people do not mind receiving alerts that inform them about threats that have a direct im- pact on them, no matter how frequently they are issued. They do object to receiving re- dundant alerts about a single event or frequent alerts about events that do not affect them (see "county-level geo-targeting" above). EMA policies should reflect the impact of alert fatigue in defining criteria for issuing WEA messages. While WEA contains no mechan- ism to track the number of people who opt out of the WEA service, EMAs should track public response by gathering information about calls and complaints to emergency opera- tions after sending WEA messages. This information may suggest future modifications to EMA policies about WEA.

Lesson 5: Addressing the Strengths and Weaknesses of WEA Geo-targeting

The WEA service not only reaches large numbers of people during an emergency but also reaches the *right* people during that emergency. Through geo-targeting, WEA messages are sent to the people in the area affected by the emergency. This makes WEA a very effective tool for alerting populations to events that cover a large area (e.g., hurricanes, snow storms, floods, hazardous chemical clouds) but less useful for localized emergencies (e.g., tornadoes, chemical spills, gas leaks).

As noted in Lesson 4, current WEA specifications require the CMSPs to disseminate alerts only at the county level. This results in alerts being sent to many people outside the area directly impacted by the emergency. Thus, the WEA service is likely to be used only for emergencies that affect a large area. For localized emergencies, the EMA must strike a balance between over-alerting large numbers of the populace and the public safety of those affected by the emergency.

Many CMSPs are already supporting geo-targeting of smaller areas, some down to the area covered by a single cell tower. EMAs should consult the CMSPs in their area to determine available geo-targeting resolution.

Lesson 6: Focusing on Creating Understandable Messages

WEA messages may not exceed 90 characters. Additionally, they may not contain telephone numbers or URLs. This is to prevent overloading telephone and computer networks with a spike in traffic after a WEA message.

The WEA message goes through several translations between the alert originator and the member of the public receiving it, as shown in Figure 4. The alert originator must understand this process to ensure the dissemination of effective alerts.

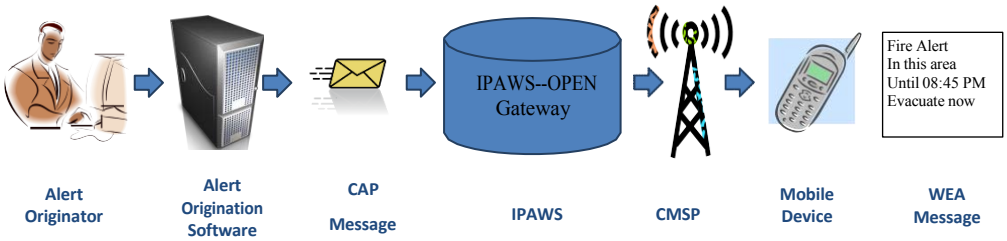

Figure 4: WEA Message Transfer

If the alert originator is not skilled at creating WEA messages, unclear messages and unacceptable delays during an emergency may ensue.

WEA messages may be generated using two methods. As a default, IPAWS-OPEN will assemble a WEA message using data from CAP fields, as shown in Table 1.

Table 1: IPAWS-Generated WEA Message Examples

CAP Field	Content	Result
Urgency	"Immediate" or "Expected"	Required to issue a WEA Message
Severity	"Extreme" or "Severe"	
Certainty	"Observed" or "Likely"	
Event Code	FRW	WEA Message
Event Category	Fire	
Expiration	2013-02-12T16:49:00-05:00 Date: 12-Feb-2013; Time: 4:49 PM; Zone: EST	Fire Warning In this area Until 4:49 PM Evacuate now
Response Type	Evacuate	

CAP Field	Content	Result
Urgency	"Immediate" or "Expected"	Required to issue a WEA Message
Severity	"Extreme" or "Severe"	
Certainty	"Observed" or "Likely"	
Event Code	HMW	WEA Message
Event Category	Safety	
Expiration	2013-02-12T08:23:00-08:00 Date: 12-Feb-2013; Time: 8:23 AM; Zone: PST	Hazardous Materials Warning In this area Until 8:23 PM Take shelter now
Response Type	Shelter	

To create a readable message, the alert originator must understand how IPAWS-OPEN assembles the message so that he/she can fill the CAP message fields with appropriate data to create an understandable message. As shown in Table 1, the primary CAP fields that contribute to message formation are the "Event code", the "Response type", and the "Expiration" fields. Mapping of these fields to the resulting WEA message is shown in Table 2.

Table 2: Mapping CAP Codes to WEA Message Text

"EVENT CODE" FIELD	
CAP input	**WEA Message Text**
AVW	Avalanche Warning
CDW	Civil Danger Warning
EQW	Earthquake Warning
FRW	Fire Warning
HMW	Hazardous Materials Warning
LEW	Law Enforcement Warning
NUW	Nuclear Power Plant Warning
RHW	Radiological Hazard Warning
VOW	Volcano Warning
AVA	Avalanche Watch
CAE	Child Abduction Emergency
CEM	Civil Emergency Message
LAE	Local Area Emergency
TOE	911 Telephone Outage Emergency

"RESPONSE TYPE" FIELD	
CAP input	**WEA Message Text**
Shelter	Take shelter now
Evacuate	Evacuate now
Prepare	Prepare for action
Execute	Execute action
Avoid	Avoid hazard
Monitor	Monitor radio or TV

"EXPIRATION" FIELD	
yyyy-mm-ddThh:xx:ss-zz:zz	
yyyy = year	mm = month
dd = day	hh = hour
xx = minute	ss = second
zz:zz = time zone	

Knowledge of this mapping will assist the alert originator in creating a CAP message that produces the desired alert. However, in many cases the alert originator is not developing the CAP message directly, but is using the user interface of alert generation software to create the CAP message. In these cases, the alert originator must understand how the alert generation software inputs map to the CAP message and/or the WEA message. This information should be obtained from the supplier of the alert generation software.

An alternate means of constructing a WEA message is to use CMAMtext, as shown in Table 3. Note that this option requires authorization from FEMA.

CMAMtext enables the alert originator to create a 90-character WEA message independent of the CAP fields cited above. While this method requires some additional skills from the alert originators, it offers the advantage of customizing a WEA message to meet a specific need.

Table 3: CMAM text-Generated WEA Message Examples

| | | |

affected area. In addition, WEA does not require a subscription, so everyone is automatically enrolled. The return can be measured in lives saved.

EMAs can evaluate this return against the investment required, which is small. The WEA distribution service itself is provided free of charge by FEMA and the CMSPs. There is no cost to enroll in the system or to use it. The only costs borne by the originator are:

- The cost of the effort to obtain authorization to use WEA
- The cost of getting, using, and supporting alert origination software The cost of training personnel to use that software

Lesson 8: Performing Public Outreach

To ensure that initial alerts are well received, it's important to inform both the public and public safety officials about WEA before issuing alerts.

- *Public Awareness:* To inform the public, EMAs should mount a publicity campaign that utilizes local media, including newspapers, television news, and radio news, as well as other available communication channels (e.g., website, Facebook, Twitter). EMAs should use these channels to inform the public regarding:
    - What the WEA service is
    - How WEA works
    - How alerts are presented
    - Privacy concerns for WEA
    - When alerts will be issued
    - How they should respond to alerts
- *Public Safety Awareness:* EMAs should create materials to inform public safety officials within their jurisdiction about the planned use of WEA. This will prepare them for possi- ble reactions to WEA messages. For example, if an EMA issues a WEA message, the lo- cal 911 call center, police department, or fire department may receive calls with questions about the alert. Preparing them in advance will enable a coordinated and consistent re- sponse. EMAs may also consider periodically reinforcing this outreach to the public after adoption of WEA. This can help ensure that the public remains aware of WEA and knows what to do when they receive an alert.

EMAs should also establish a mechanism to notify public safety and emergency management agencies in neighboring jurisdictions about the planned use of WEA. Due to county-level geo-targeting and message bleed-over, residents in those jurisdictions may see WEA messages issued by the EMA. The officials in these jurisdictions must be prepared to field questions from the public. EMAs may want to establish coordination policies and procedures with these neighboring jurisdictions.

3 Conclusion

In December 2011, NYC OEM, in collaboration with DHS S&T, FEMA, FCC, and local CMSPs, successfully demonstrated the WEA service by disseminating demonstration alerts throughout the New York City metropolitan area. This was the first significant application of the WEA service and served to demonstrate the ability of WEA to enhance public safety. It also identified some challenges that EMAs will face in adopting and utilizing WEA.

The authors have studied the activities of the demonstration participants in preparation for this demonstration, interviewed those participants, and researched the operational characteristics of WEA, to identify the following eight lessons learned from the demonstration:

1. Coordinating Across Alerting Agencies
2. Considerations for Choosing Alert Origination Software
3. Building and Maintaining Proficiency
4. Factors to Consider Before Sending a WEA Message
5. Dealing with the Strengths and Weaknesses of WEA Geo--targeting
6. Focusing on Creating Understandable Messages
7. Justifying Your Investment in WEA
8. Performing Public Outreach

These lessons are presented in this report, and address activities and challenges that many EMAs adopting WEA can expect to face. The lessons provide EMAs with the ability to learn from the NYC demonstration.

Appendix A Interview with Mark Frankel

NYC OEM derived a number of lessons from its adoption and demonstration activities. The agency's experiences offered organizational learning in the areas of resources, staff buy-in, outreach, technology, SOPs, and staff training. These lessons are presented in the following interview with Mark Frankel.

Q1. Overall, what were the primary takeaways from your experience adopting the WEA service? What can other emergency management agencies learn from your experience?

Frankel: NYC OEM completed its WEA adoption activities under unusual circumstances that will not affect other alert originators seeking to adopt WEA. Many of our challenges arose from our need to deploy the system before FEMA and the CMSPs were ready. For alert originators looking to adopt WEA now, getting online with WEA will be much easier-FEMA provides a great overview of the process for becoming an alert originator on their website [FEMA 2012a]. There are many AOSPs who are rolling out WEA-compatible software. That said, you need to think about how WEA fits into your existing alerting practices before moving forward with the decision to adopt WEA and completing FEMA's four-step process for becoming an IPAWS alerting authority.

Although most WEA adopters will not perform a system demonstration like we did, we learned a lot from it. For the most part, the system worked well-the messages flowed from NYC OEM, to IPAWS-OPEN, to cell towers, to volunteers' mobile phones. The speed with which volunteers received the alerts underscored the value of using WEA during an emergency event. We also learned more about the geo-targeting capabilities of WEA. The demonstration message intended for all five boroughs reached the five boroughs. The demonstration messages intended for individual boroughs reached each borough. We did see some bleed-over across borough borders. This reinforced the importance of making WEA message content applicable to an entire borough and to indicate the affected zip code in the message.

Q2. Why did NYC OEM choose to adopt the WEA service?

Frankel: We saw WEA as a valuable tool not only to reach large numbers of people during an emergency but also to reach the *right* people during that emergency. We have a large permanent population in the city. We also have an even larger number of visitors each year. Prior to WEA, we had several ways of reaching these people. One way was through the media, issuing alerts via television and radio. These reach a lot of people-the entire New York metropolitan area-but they're not targeted to just the people affected by the emergency. If there is a hazardous material spill affecting two streets in Lower Manhattan, do we want to issue an alert to all five boroughs? If we do that too of-

ten, people will become desensitized and may ignore future alerts that do pertain to them. Because of this, we don't issue city-wide alerts very often.

The other way we can alert the public is through our Notify NYC service. This service alerts people via text messages, voice messages, and email. But the alerts go only to people who have subscribed to the service, which constitutes just a small fraction of the permanent population, and virtually none of the transient population. We also use social media, such as Twitter and Facebook, but the percentage of the population alerted by these means is also small.

WEA is unique. It is a not a subscription service, so unless people take action to opt out, everyone is automatically enrolled. And it is a geo-targeted service, enabling us to send alerts just to the area affected by the emergency. Right now, the WEA specification for geo-targeting requires the CMSPs to disseminate alerts only at the county level. This is too broad. It gets us back to the same problem with alerting people via the media. You end up alerting a lot of people who are not affected by the emergency. But I have hope that the relevant federal agencies and CMSPs will soon enhance WEA to enable geo-targeting to much smaller areas, like a few city blocks. When that happens, WEA will become a really valuable alerting tool for us.

Q3. Was it difficult to obtain alerting authority?

Frankel: There are a couple of steps to this process [FEMA 2012a]. First, we needed to determine which public alerting permissions to apply for. We coordinated with other agencies in and around our jurisdiction, such as our local NWS office, to define the scope of our alerting authorities. We concluded that we should apply to issue Imminent Threat Alerts only, including both non-weather and weather-related events.

We then had to go through FEMA's four-step application process. The first step was to get software to generate the alerts. The software had to be certified by FEMA as IPAWS compatible. Second, we applied for an MOA. The MOA governs system security and was tailored to our organization and the software we had chosen. Third, we applied for public alerting permissions for the types of alerts that we wanted to issue. We had to have this application approved by New York State prior to submitting it to FEMA. We had to do a little research to identify the appropriate state agency to contact. I expect this step will become easier for alert originators as more get online with WEA and each state solidifies its procedures. Finally, we had to complete the FEMA IS-247 training course, which provides web-based IPAWS training.

Q4. You needed to obtain IPAWS-compatible software to generate WEA messages. Given your experiences, do you have any recommendations for other alert originators?

Frankel: We were an early adopter, and many of our challenges resulted from being first. We had few options for obtaining software, and the available products were still in development. Alert originators looking to adopt WEA now have an increasing number of

certified suppliers to choose from on FEMA's IPAWS-OPEN Developers list, which is available on FEMA's website [FEMA 2012c].

Clearly, you need to choose a product or service that meets the technical needs of the WEA service-it must be CAP compliant and IPAWS-OPEN compatible. But you also need to make some decisions about how you plan to use WEA. What kinds of alerts do you want to issue? Imminent Threat Alerts? AMBER Alerts? Do you want to construct your own messages using CMAMtext, assuming you can get permission from FEMA to do so, or do you want to let IPAWS-OPEN assemble your messages from the various CAP fields? Do you want to draft each message, or do you want to use standardized templates? Whatever you decide, it's important to communicate these decisions to the AOSP to ensure that the provider delivers a satisfactory system.

You might also prefer a system that integrates WEA with your other alerting capabilities over a stand-alone solution. Using CAP, you can create one message and push it out to all the appropriate dissemination channels. Also, with several stand-alone tools, staff members will need to monitor multiple systems.

Security is another key factor to consider. You don't want your system to get hijacked, enabling some hacker to broadcast alerts throughout your jurisdiction. The digital certificates issued by FEMA prevent unauthorized access to IPAWS-OPEN. IT security measures within NYC OEM prevent access of our systems by outsiders. And within OEM, our systems ensure that only authorized and authenticated users have system access.

You need to consider other business needs, too. You want a system that will be familiar to your users, a system with a user interface similar to what they already have. So the user interface will be a major discriminating factor among the potential suppliers. You need to choose one that supports the manner in which your agency operates and the way your staff is trained. Many AOSPs are developing IPAWS-compatible software now. Talk with your current AOSP to see what the provider has planned. It may be an easy extension to what you are already using. That would facilitate compatibility with your existing systems and operations.

And don't forget about system support. Do you want a hosted solution that resides on your servers, or do you want a remote service? If you host the system, you need to ensure that it is supported, updated, and so forth. If you subscribe to a service, the provider will take care of those things but also must deliver the level of service that you require. In a real emergency, will you be able to access the service through jammed communication channels?

Q5. What challenges did you face when establishing an MOA with FEMA?

Frankel: Not many. There is a simple form to fill out, and it's available on FEMA's website [FEMA 2012e]. Alert originators need to list their primary alert origination software and all the systems they have that will interface with IPAWS-OPEN. We also

checked whether we needed to submit a separate MOA for each of the AOSP products that we planned to use to originate WEA messages for the demonstration-we did not.

Q6. You mentioned that NYC OEM had to consider how the WEA service would fit **into NYC OEM's existing processes. Can you tell us more about that?**

Frankel: From my perspective, it's more important for an organization to begin with effective alerting practices, then determine which dissemination channels to use to reach the public. NYC OEM is a large emergency management agency, and we have dedicated staff, our public warning specialists (PWSs), to issue alerts to the public. All PWSs do is issue alerts. They drill constantly to prepare for crafting effective alert messages and issuing alerts during emergency events. During an emergency, they are at hand to write and send alerts, ensuring that the public receives the information quickly and has time to react. When NYC OEM adopted WEA, we had already operationalized alerting within the agency. So for us, adopting WEA was relatively easy: we completed FEMA's four steps for becoming an IPAWS alerting authority, we upgraded our SOPs to incorporate WEA into our existing processes, and we had plenty of staff to support the effort.

Smaller agencies with more limited resources may not have staff dedicated solely to issuing alerts and may not have operationalized alerting within their organizations. They'll have to spend more time up front planning for WEA adoption. The fact that an alert originator no longer needs to rely on a subscriber base and can reach both residents and visitors in a county is one of the truly great benefits of WEA, but it's important to consider how that capability will fit into an agency's procedures before taking the first steps to adopt WEA.

Q7. How did you go about developing SOPs for the WEA service?

Frankel: We needed to ask ourselves a lot of questions about our alert origination process. How would WEA fit into our existing alerting processes? Which staff members would issue WEA messages during an event, and how quickly could they do it? And how would the system's ability to geo-target WEA-capable mobile phones at the county level with a 90-character alert message enhance our existing public alerting capabilities?

For NYC OEM, Commissioner Bruno's objective in adopting WEA was to integrate it as another tool in the agency's toolbox; he wanted one more alert communication pathway at our disposal during an emergency. So we knew WEA would not replace any other tool or communication pathway and that our existing staff of PWSs would issue WEA messages just as they do for our other alert dissemination pathways. We also needed to know what level of certainty about an emergency event would trigger issuing a WEA message, who to notify internally or externally before issuing the alert, and how to construct an effective 90-character alert message. Waiting until an actual emergency to determine these answers would delay the public's receipt of a WEA message, thus decreasing its value.

Our Operations Division, which includes our staff of PWSs who are the primary users of WEA, led the task of incorporating WEA in our SOPs. We consulted our existing SOPs

to determine how WEA's capabilities fit into the agency's existing alert toolbox. As part of this analysis, we examined a long list of past emergency events during which the agency had issued an alert through one or more of our other communication pathways, such as Twitter and SMS text messaging. We then identified the instances in which a WEA message would have been valuable. We considered the WEA guidelines provided in FEMA's IS-247 course training regarding the appropriate use of message components, CAP elements, event codes, and message templates. We also looked at the demonstration data from December and what it taught us about WEA's capabilities and limitations-namely, the 90-character text limit, geo-targeting specifications, and bleed-over probability. Finally, we considered how our public responds to alert messages and designed our WEA-specific SOPs to avoid instances of over-alerting where possible.

Q8. How do you handle the county-level geo-targeting resolution of the WEA service?

Frankel: NYC OEM will not issue WEA messages below the county level because one of the major CMSPs in our area will not target below this level right now. From our perspective, this limits the usefulness of WEA. Each of the city's five boroughs-Brooklyn, Bronx, Manhattan, Staten Island, and Queens-functions as a separate county. Their populations range from approximately 400,000 in Staten Island to 2.5 million in Brooklyn, and these figures do not account for the hundreds of thousands of visitors who may be in any one of the five boroughs at a particular time. Furthermore, the boroughs range in physical size from Manhattan's 23.7 square miles to Queens's 112.2 square miles. When developing our SOPs, we had concerns that alerts issued at the county level would reach many people who would not be affected by a particular emergency event. We had to consider several resulting scenarios, one being that a large number of people would opt out of WEA if they received messages that did not affect their immediate location. Another is that the specificity of message content would be limited because all message recipients within a borough may not be able to take the same action. For example, the WEA message "evacuate south" may help borough residents downwind of a chemical spill but may cause harm to borough residents upwind of the chemical spill. The potential confusion or harm that results from issuing the same protective-action information to all geographic sections of a borough, or from message bleed-over into additional boroughs, limits our current use of WEA.

So we designed our SOPs to minimize the number of people who receive a WEA message. In essence, we issue WEA messages only for the most urgent and severe emergencies, when the benefit of reaching members of the public in need of urgent information outweighs the detriment of alerting members of the public not affected by the event. While we cannot track the number of people who choose to opt out of WEA messages, we do intend to track public response by gathering information about calls and complaints to 911 and 311 after sending WEA messages. This information may lead us to modify our WEA use guidance in the future. The opt-out problem is of real concern to us. Once someone opts out, we may never get them back. I suggest to FEMA that it would be a good idea to require people to renew their opt-out decision annually.

As we learned from the December 2011 demonstration event, geo-targeting WEA messages at the county level challenges our PWSs to maintain spatial awareness about borough and city borders. They must understand that issuing a WEA message to one borough may result in message bleed-over to WEA-capable mobile phones in an adjacent jurisdiction, such as a neighboring New York City borough or a neighboring county in New Jersey. Because message bleed-over is possible any time we issue a WEA message, our SOPs account for the need to coordinate with a larger number of public safety officials than is required when using one of our other tools, specifically Notify NYC, which can target single zip codes.

We also decided to include the zip code of the area affected by an emergency event, when possible. The zip code will improve the public's understanding of an emergency event's impact and the specific areas within a county that should take action to avoid an imminent threat. We also continue to explore how to address the current geo-targeting challenges, such as originating multiple WEA messages to the same borough to address different geographic sections of it. But for now, we foresee that the limits of geo-targeting will continue to restrict the WEA service's use in New York City until all the major CMSPs can disseminate WEA messages at a more granular level.

Q9. How do you plan to deal with the 90-character limit?

Frankel: WEA provides two ways to generate messages. You can fill out the appropriate fields in the CAP message, and IPAWS-OPEN will assemble them into a WEA message. The other method is to directly author the WEA message using a CAP field known as CMAMtext. We opted to use the CMAMtext field to create our own 90-character messages; this allowed us to issue messages clearly marked as "test" during the demonstration event and now gives us greater control in exactly how we craft our WEA messages. But I'm not sure that this option will be available to all originators. A formal CMAMtext standard does not yet exist. Right now, FEMA treats CMAMtext as an experimental feature during this initial stage of WEA deployment and grants only a limited number of alert originators the ability to use it.

If you are able to create your own 90-character messages, you need to decide how you will do that. We're a large organization. We have a number of alert specialists who develop and maintain a proficiency in alert authoring. Because of this, we write individual messages for each emergency event that we alert the public about. We use daily drilling to hone the PWSs' abilities to create these messages within the 90-character constraint.

This approach may not be practical for smaller agencies that do not have dedicated alert originators. In such cases, it may be difficult to maintain the needed proficiency. An alternative approach would be to create a collection of message templates that alert originators could easily tailor with information specific to events.

Whichever method you choose, make sure that your AOSP knows this is your agency's approach and will deliver the capabilities to support it. And remember that training and drilling is important to maintain the necessary proficiency with either approach.

Q10. Given all that, under what circumstances will you use the WEA service?

Frankel: We intend to use WEA for only the most urgent and severe emergencies because geo-targeting at the county level means that many people receiving the message probably will not be affected by the event, unless it is a county-wide event. We want to avoid message fatigue as much as possible to reduce the number of people who opt out of WEA or simply begin ignoring alert messages.

Every incident is different, and our guidelines for using the communication pathways are flexible so that PWSs can tailor their communication with the public to the impact of the incident. We do not say, for example, "We'll always use WEA for flooding and never for chemical spills." As with any other tool in our alerting toolbox, our procedures for using WEA depend on the anticipated impact of the incident. Our SOPs direct our PWSs to use WEA as a "whistle blower" to raise the public's awareness about an emergency incident and direct people to take specific action to avoid harm.

Our SOP analysis and updating exercise led us to identify specific event *types* for which our PWSs *should consider* using WEA as that whistle blower:

- an emergency incident expected to cause other emergencies
- an emergency incident with a wide geographic impact and severe or extreme result
- an emergency incident with a limited geographic impact and severe or extreme result
- an emergency incident that may overburden the 911 system as a result of the public's increased level of concern, need to report information, or need to gather information
- an emergency incident that requires all or a portion of the public to evacuate, shelter in place, or take other preventative action

We can use WEA this way because we still use all the other alerting pathways that we had before we adopted WEA, including EAS, Notify NYC, and social media such as Twitter. We simply re-ranked these communication pathways based on incident severity, now accounting for WEA, as a result of our SOP analysis and updates (see Figure 5).

Figure 5: NYC OEM's Communication Pathways Ranked by Severity [adapted from NYC OEM 2012]

Basically, our PWSs use Twitter for the least severe incidents, such as a subway service restoration. And we reserve EAS for the most severe incidents. The greater the severity of an incident, the greater the number of communication pathways we use to communicate information to the public. Our PWSs use the highest communication pathway first, followed by the communication pathways below it. This ranking process also means that the PWSs send a tweet for every alert or notification message that they issue. For example, we may categorize an event as a mid-level incident due to its limited geographic impact and moderate potential to cause harm. In this case, the PWSs would first send text messages to local residents via Notify NYC, then they would send email messages via Notify NYC, and last they would send a tweet about the incident via Twitter.

Q11. How would an alert originator go about convincing an organization's management of the value of the WEA service?

Frankel: Well, that wasn't a problem that we faced. Our management started the effort to adopt WEA, so there was no convincing to be done. But if we had to convince them, I don't think that it would have been very difficult. WEA has a pretty good return on investment. The return can be measured in lives saved. If you can alert people about a flash flood, a tornado, or a toxic chemical spill and get them out of harm's way, you can save lives. WEA is an effective means to do that. It gives you the opportunity to reach a large number of people very quickly.

You can then evaluate this return against the investment required, which is pretty small. The WEA service itself is provided free of charge by FEMA and the CMSPs. There is no cost to enroll in the system or to use it. The only costs borne by the originator are the cost of the effort to obtain authorization to use WEA, the cost of getting and using alert origination software, and the cost of training personnel to use that software. If you integrate WEA into your existing alerting capabilities, these costs can be very small.

Q12. What kind of outreach did you do before adopting the WEA service?

Frankel: It's important to inform both the public and public safety officials about WEA before issuing alerts. If you don't, your first alert will not be well received. We created awareness materials to inform the public as well as public safety officials in the city and in surrounding jurisdictions about this service. This outreach also highlighted the need for us to circle back with colleagues once we completed our adoption activities. At that point, we issued a bulletin to the city's key public safety agencies: the New York City Police Department, New York City Fire Department, and New York City Hall. We also sent the bulletin to the New York State Office of Emergency Management and surrounding jurisdictions' 911 call centers in New York and New Jersey to let them know that NYC OEM would use WEA to alert the public during some emergency events.

Some jurisdictions may want to consider periodically reinforcing their outreach to the public once they adopt WEA. This can help ensure that members of the public in a juris-

diction know what to do when they receive WEA alerts on their mobile phones. For NYC OEM, we felt satisfied that the information we provided to the general public in our initial press release was sufficient and completing adoption activities didn't warrant conducting additional public outreach when we deployed WEA. We also see that the CMSPs are conducting outreach to the public via their websites and retail materials included with WEA-capable mobile phones. So we expect that between these two activities, the public has a sufficient amount of information about WEA given how we intend to use the system right now.

Q13. How did you train your staff to use the WEA service?

Frankel: We used FEMA's IS-247 training course. The course offers a good overview of IPAWS, how to compose messages in CAP, and how to write an effective message. Although FEMA requires only one representative from each COG to participate in the training, we decided to require all of our PWSs to take the course to give everyone a baseline understanding of WEA. I serve as the point person who ensures all the PWSs take the training by maintaining each PWS's IS-247 training certificate. Each PWS must have a certificate on file before I grant the individual access to the software for issuing WEA messages.

In addition to everyone taking the FEMA training course, we also developed NYC OEM-specific training and materials that cover our agency's SOPs and our IPAWS-compatible software.

Alert originators should also make sure that their AOSP will provide training on the operation of their system. Creating a short how-to manual illustrated with screenshots would be a good idea.

Q14. How did you develop your training materials?

Frankel: I had a lot of experience developing and testing the IPAWS-compatible software with the AOSPs, so I had a pretty intimate knowledge of the new WEA service. That helped me create in-house training materials that reflected both the tool's steps for issuing an alert and our agency's SOPs for WEA.

I took an iterative approach to produce the training materials. I developed the training and gave it to the Operations Division staff and our PWSs, who issue the WEA messages. The PWSs then provided their feedback on the training to me, and I used the feedback to upgrade the training, redelivered it to the PWSs for more feedback, and continued to tweak the materials until we were all satisfied with the approach and content of the training.

Q15. Does NYC OEM plan to conduct any kind of annual training of staff?

Frankel: Our staff complies with the rules of behavior stipulated in our MOA with FEMA; this requires all staff who use IPAWS-connected systems to participate in annual IT security awareness training. Otherwise, we believe FEMA's IS-247 training, which all

of our PWSs take once, is sufficient, and we don't plan to conduct annual training focused specifically on WEA or IPAWS.

That said, WEA's comparatively limited message size and content challenges our PWSs to create alerts that are useful to the public. We address this challenge by requiring our PWSs to drill virtually on a daily basis: they practice drafting WEA message text for every incident for which the agency issues an alert, regardless of which communication pathway they actually use to disseminate that alert. And we have the PWSs practice issuing WEA messages on the agency's compatible software to ensure that they are comfortable using the software's interface.

We derived the practice of boiling down every alert message to the limited number of characters required by each of NYC OEM's alert communication pathways from our experience adopting Twitter as a communication pathway. Twitter allows a maximum of 140 characters. So first the PWSs learned to write messages within 140 characters; now they practice doing so for 90 characters. This ensures that a PWS's WEA message origination skills stay sharp regardless of how often we actually originate a WEA message for the public.

Q16. The end-to-end demonstration was obviously valuable to FEMA and the CMSPs. What did your organization gain from doing the demonstration in your jurisdiction?

Frankel: During the demonstration, we uncovered previously unknown system connection and software issues that the demonstration partners needed to resolve before WEA went live in New York City. It also helped us understand more about the WEA service's current geo-targeting capabilities. For example, data demonstrated some bleed-over across boroughs. This data influenced our SOP development because it underscored the need to make WEA message content applicable to an entire borough, rather than to a smaller area within a borough. The demonstration also showed us how different brands of WEA-capable mobile phones present WEA messages due to variations in screen display, sound, and device specifications. Press officers will use these data to inform any outreach and public education activities that they conduct in the future.

Jurisdictions should consider testing WEA before officially deploying the system. An internal test will tell you whether your staff knows how to use your IPAWS-compatible software, that the software works as you expected it to, and that you have established your connection to IPAWS. It may also expose gaps in your SOPs, which you can address by revising them to include procedures specific to WEA. An external test, one that sends a test message to the public, will give you information about geo-targeting accuracy and bleed-over, but every jurisdiction may not need to do this. And this kind of testing may not always be possible due to restrictions from the FCC. As more and more organizations adopt, test, and use WEA, testing the WEA service from IPAWS to the CMSP gateways and their customers' mobile phones may become less necessary.

Q17. What resources outside of NYC OEM were most valuable to your WEA adoption activities?

Frankel: Our adoption of WEA began so early because New York City officials were highly motivated to obtain this service for the public in our city. As a result, NYC OEM's own leadership as well as the Mayor's Office was supportive in helping us with activities like finding the right contacts for state approval of WEA authority and escalating reviews of press releases and legal documents. Alert originators should try to get buy-in from their local officials as they begin the adoption process. Our local officials proved helpful in connecting us with other local and state government resources who helped cut through the red tape during some adoption-related activities.

Our colleagues in neighboring jurisdictions, including the local NWS office, helped with our efforts. We needed to coordinate with them to decide which alerting authorities to apply for and to make them aware of our activities so that they could prepare for alert bleed-over. Alert originators will need to keep these two things in mind. You want to avoid jurisdictional overlap in alerting authority because conflicting alert messages could confuse the public. And you want to have close relationships with neighboring jurisdictions so that you can coordinate activities during emergencies.

We also had direct access to a representative from FEMA to ask questions about the adoption process, becoming an IPAWS alerting authority, and connection issues that we and our AOSPs experienced as we tested our new origination software internally. Alert originators adopting WEA now can find a wealth of information on FEMA's IPAWS website, such as instructions on how to sign up for IPAWS, a link to the MOA application, and an e-learning course called IS-247.A about IPAWS [FEMA 2012d].

And the four major CMSPs in our region all worked with us to help us understand each provider's cell tower coverage, timeline for upgrading coverage, and the provision of mobile phones for testing. Alert originators should contact their jurisdiction's primary CMSPs to discuss whether they are IPAWS authorized, at what level of geo-targeting granularity they will disseminate WEA messages, and how they are educating their customers about WEA.

Q18. As we wrap up, is there anything you can think of that you would have done differently? Do you have any final recommendations for other alert originators considering or planning for WEA adoption?

Frankel: I would like to see more outreach to the public about what WEA is and what to expect from it. Education should start at the point of sale; retailers should talk to customers about WEA when they buy their phones. They should know that the WEA message will inform them of an emergency event but cannot give them all the details in 90 characters. They'll still need television, radio, or the internet for that.

For alert originators getting ready to adopt WEA, develop your SOPs before you start thinking about dissemination channels. Once you've operationalized alerting procedures

inside your organization, you can create good alerts, regardless of the method you use to send them. It helps to have someone whose primary job is to write and format the alerts, if the organization's size allows for that.

I would also encourage all alert originators to start using CAP if they don't already. If your alert messages are CAP compliant, you can construct one message and disseminate it through all your other alerting channels. And if your organization is already CAP compliant, going one step further to integrate WEA should be simple. When you talk to your software providers, ask whether they are CAP compliant, and write this requirement into your requests for proposals and contracts.

But the main thing is that other alert originators will have an easier time adopting WEA now that the IPAWS architecture is developed and procedures have solidified. WEA is a great addition to the nation's public alerting system, and it will help us reach people both at home and on the go in a way we never could before.

Appendix B List of Acronyms

Term	Definition
AMBER	America's Missing: Broadcast Emergency Response
AOSP	alert origination service provider
CAP	Common Alerting Protocol
CMAM	Commercial Mobile Alert Message
CMAS	Commercial Mobile Alert Service
CMSP	commercial mobile service provider
COG	Collaborative Operating Group
DHS	Department of Homeland Security
EAS	Emergency Alert System
EDXL	Emergency Data Exchange Language
EMA	emergency management agency
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
IPAWS	Integrated Public Alert and Warning System
JITC	Joint Interoperability Test Command
MOA	memorandum of agreement
NWS	National Weather Service
NYC OEM	New York City Office of Emergency Management
OASIS	Organization for the Advancement of Structured Information Standards
OPEN	Open Platform for Emergency Networks
PLAN	Personal Localized Alerting Network
PWS	public warning specialist
RSS	Really Simple Syndication
S&T	U.S. Department of Homeland Security Science and Technology Directorate
SMS	short message service
SOP	standard operating procedure
WEA	Wireless Emergency Alerts

References and Resources

URLs are valid as of the publication date of this document.

[CFR 2012]
Code of Federal Regulations. *Part 10: Commercial Mobile Alert System* (47 CFR 10 §1-540). Washington, DC: U.S. Government Printing Office, 2010-2012.

[FCC 2008]
Federal Communications Commission. *CMAS Third Report and Order* (FCC 08-184, PS Docket No. 07-287). Washington, DC: FCC, 2008. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-184A1.pdf

[FCC 2012a]
Federal Communications Commission. *Commercial Mobile Telephone Alerts (CMAS)*. Washington, DC: FCC, 2012. http://transition.fcc.gov/pshs/services/cmas.html

[FCC 2012b]
Federal Communications Commission. *Master CMAS Registry*. Washington, DC: FCC, 2012. http://www.fcc.gov/pshs/docs/services/cmas/MasterCMASRegistry.xls

[FEMA 2012a]
Federal Emergency Management Agency. *Alerting Authorities*. Washington, DC: FEMA, 2012. http://www.fema.gov/alerting-authorities

[FEMA 2012b]
Federal Emergency Management Agency. *Commercial Mobile Alert System*. Washington, DC: FEMA, 2012. http://www.fema.gov/commercial-mobile-alert-system

[FEMA 2012c]
Federal Emergency Management Agency. *IPAWS OPEN Developers*. Washington, DC: FEMA, 2012. http://www.fema.gov/library/viewRecord.do?id=5670

[FEMA 2012d]
Federal Emergency Management Agency. *IS-247.a: Integrated Public Alert and Warning System (IPAWS)*. Washington, DC: FEMA, 2012. http://training.fema.gov/EMIWeb/IS/is247a.asp

[FEMA 2012e]
Federal Emergency Management Agency. *Memorandum of Agreement*. Washington, DC: FEMA, 2012. http://www.fema.gov/library/viewRecord.do?id=6019

[Mileti 1991]
Mileti, Dennis S. & Fitzpatrick, Colleen. "Communication of Public Risk: Its Theory and its Application." *Sociological Practice Review 2,* 1 (1991): 20-28.

[Mileti 2000]
Mileti, Dennis S. & Peek, Lori. "The Social Psychology of Public Response to Warnings of a Nuclear Power Plant Accident." *Journal of Hazardous Materials 75,* 2-3 (June 2000): 181-194.

[NYC DOITT 2012]
New York City Department of Information Technology and Telecommunications. *Policy and Strategy: IT Policy & Governance.* New York: DoITT, 2012. http://www.nyc.gov/html/doitt/html/policy/it_policy.shtml

[NYC OEM 2011]
New York City Office of Emergency Management. "Office of Emergency Management Advises New Yorkers About Upcoming Test of Wireless Emergency Alerts for Mobile Phones" (11-27) [Press release]. New York: NYC OEM, December 4, 2011.

[NYC OEM 2012]
New York City Office of Emergency Management. http://www.nyc.gov/html/oem/html/home/home.shtml (2012).

[Office of the Mayor 2011a]
Office of the Mayor. "Mayor Bloomberg Announces New York City Drew a Record-Breaking 48.7 Million Visitors in 2010" (PR-003-11) [Press release]. New York: Office of the Mayor, January 4, 2011a.

[Office of the Mayor 2011b]
Office of the Mayor. "Mayor Bloomberg, the Federal Communications Commission, the Federal Emergency Management Agency and Wireless Provider Executives Unveil New, First-in-the-Nation Emergency Notification Service That Will Reach Mobile Devices Located in Affected Areas" (PR-146-11) [Press release]. New York: Office of the Mayor, May 10, 2011b.

[U.S. Census 2012]
U.S. Census. *State and County Quickfacts: New York (City), New York*. Washington, DC: U.S. Census, 2012. http://quickfacts.census.gov/qfd/states/36/3651000.html