What every emergency manager needs to know about CAP alerting . . . (but was afraid to ask)

By Mark O'Brien
SpectraRep

SpectraRep
BIA fn SOLUTIONS FOR EMERGENCY MANAGEMENT AND PREPAREDNESS

November 2010

Contents

Executive Summary

On September 30, 2010 the Department of Homeland Security's Federal Emergency Management Agency (FEMA) officially adopted the Common Alerting Protocol (CAP) for all national level alerts. This mean that all broadcast radio and television stations must be able to receive and process a CAP alerting file and be able to use that CAP alert to trigger their existing EAS equipment at by September 30, 2011.

For state and local alert and warning this means that the future is digital and will be CAP based. Broadcast stations are not unplugging their legacy EAS equipment, but they now must also be able to receive a CAP file to trigger EAS.

> *"Our goal is simple – to give one message over more devices to more people for maximum security"*
> Craig Fugate, FEMA Administrator

CAP is an XML schema, essentially a structured text file. It was developed by the emergency management community to improve alert and warning by standardizing the process of distributing all-hazard safety notifications and emergency warnings. CAP provides many benefits that are not possible in the analog world, including;

- Multiple distribution paths, eliminating the daisy chain currently in place
- Allows seamless integration with multiple receive devices
- Allows for automation of processes at the receive end
- More descriptive information can be sent along with the alert
- Message security and authentication options are enhanced
- Message creation can be simplified
- The standard can evolve as needs and opportunities change

Now that FEMA has officially adopted CAP, it is safe to assume that all broadcast stations in the country will be able to receive and process CAP files by October 1, 2011. This opens the door to standards based alerting. Other entities originating alerts and warnings can benefit from knowing that CAP alerts will pass through to the public.

Longer-term, the benefits of an all digital CAP based alerting infrastructure will lead to more efficiency, better targeting and a better informed public.

Introduction

In 2004, DHS and FEMA began a program in partnership with the National Oceanic and Atmospheric Administration (NOAA), the Federal Communications Commission (FCC), and public/private stakeholders to research how to use emerging communications technologies to improve public alerts and warnings to achieve a near instantaneous transmission.

On June 26, 2006, President Bush signed Executive Order 13407, directing the Secretary of the Department of Homeland Security to create a comprehensive Integrated Public Alert and Warning System (IPAWS) for the United States. This presidential mandate called for an integrated alert and warning system to reach as many people as possible through as many forms of communication as possible.

> *"It is the policy of the United States to have an effective, reliable, integrated, flexible, and comprehensive system to alert and warn the American people....and to ensure under all conditions the President can communicate with the American people."*
> George W. Bush, Executive Order 13407
> signed June 26, 2006

A key goal of IPAWS is to take advantage of technology advancements and marketplace developments, allowing new and innovative ways to directly reach more of the public during an emergency. A recent Cellular Telephone Industry Association (CTIA) survey found that 93% of Americans use a cell phone and that Americans trade 5 billion text messages per day[1]. Clearly, other ways of reaching out to people on the move have to be explored and integrated.

We live in a digital world. It is time our emergency alert infrastructure catches up and takes advantage of what current technology can achieve. Clearly, just moving from analog to digital is not the solution. CAP, an internationally recognized standard for alerting, is currently in version 1.2 and has been designed to adapt as technology evolves. For now CAP augments EAS, it does not replace it. That could change in the future.

History of Emergency Alerting

In the early days of alerting, radio and television were the only efficient means of reaching the general public. While radio and television are still very effective, technology has improved considerably since the first notification system was introduced in the 1950's.

In 1951, President Harry Truman established CONELRAD (CONtrol of ELectromagnetic RADiation) as the first national alerting system. Under CONELRAD, Selected radio stations provided public alerts via 640 kHz or 1240 kHz frequency, which were highlighted on all radios sold after 1953 with a CD (Civil Defense) mark, so people could quickly find the frequencies. Other radio stations were required to turn off their transmitters so that enemy bombers could not use their transmitters as beacons to target bombs.

In 1963, CONELRAD became the "Emergency Broadcast System" (EBS). The EBS was designed to provide the President with a means to address the American people over radio and television in the event of a national emergency. Through the EBS, the President had access to thousands of broadcast stations to send an emergency message to the public. The system was also expanded, with assistance from the FCC and the National Weather Service, for use in case of state, territorial, tribal, and local emergencies. The dissemination of national alerts was mandatory for broadcasters, while state, territorial, tribal, and local alerts were voluntary.

In 1994, to overcome some of the limitations of the older EBS system, the Federal Communications Commission (FCC) replaced the EBS with the Emergency Alert System (EAS). The major difference between EBS and EAS was the automatic relay method used to alert broadcast stations about an incoming message. Cable, satellite and other delivery networks were also added.

With EAS, not only the President, but national, state and local authorities were given the ability to provide emergency information to the general public via broadcast stations and cable systems. While participation in national EAS alerts is mandatory for these providers, state and local area EAS participation is voluntary.

IPAWS is the next generation of the nation's alerting infrastructure. Unlike earlier iterations, it is all digital and was originally known as the Digital Emergency Alert System (DEAS). IPAWS also improves distribution over the daisy chain system used until now and has added new IP network delivery options. IPAWS uses the Common Alerting Protocol (CAP) as the standard for all digital alerts. At the same time, IPAWS is completely backwards compatible with EAS.

As CONELRAD became EBS, which morphed into EAS, the core alert mechanism remained basically the same, an analog daisy chain from radio station to radio station. IPAWS is the first true complete infrastructure revamp in almost 60 years.

Demystifying CAP

CAP is a buzzword that has been floating around since 2001. It holds the promise of unifying alerting, dare we say standardizing alerts, but what is it? Why was this standard picked? How does it work and can it really deliver a more robust efficient future for alerting? The CAP standard was designed from inception to address these concerns.

> *"The great thing about standards is that there are so many to choose from"*
> Andrew S. Tanenbaum

What is CAP?

CAP is nothing more than a text file that has a very specific structure. You can open a CAP file in notepad or Word or even in an Internet browser. You can create one from scratch in a word processor, as long as you follow the specific schema, or design criteria.

The structure used is Extensible Markup Language (XML). XML is a way to organize information in a way that can be understood and processed by multiple devices, as long as those devices hold the key to understanding the different instructions in the file. The key is CAP, which lays out a set of shared understanding and rules. CAP is nothing more than an XML schema that details specific options within various message elements. When this

schema is understood and followed by the originator and recipient of an alert, you get clear actionable communication.

XML uses tags that identify elements of the alert, to which the message originator can assign values. In CAP, those elements quantify variables like the certainty that something will happen, the expected severity, the type of threat, the affected area, a description of the event, instructions detailing what the recipient should do, and much more.

The key to CAP's usefulness is the schema. Like all standards, it is a very strict set of rules that must be followed. If you follow the rules on both the creation and receive side processing, the possibilities become limitless.

CAP is essentially a single message format or language, spoken by multiple alerting devices. The benefit of being able to talk to alerting devices in one language is that you can send one message and know that all of the disparate receive devices will know how to respond, or if they should respond at all. CAP is great for standardizing EAS and allowing capabilities beyond what is currently possible. It really shines when all devices understand CAP and can take appropriate action based on what each sees in the CAP file.

A CAP alert file contains elements that identify the nature of the emergency event. These elements can be viewed individually or combined into a list of conditions that must be met for a receive device to take some action. For example, a roadside sign may be programmed to wake up if the response type is "evacuate", but not if it is "shelter". If all of the conditions it is looking for are not met, no action will be taken. With the elements and possible values, alert processing devices can get very granular in what action to take when a CAP file is received.

Once a CAP file has been created, it can be distributed over various and multiple paths. You can send the same CAP file to the same recipient multiple times over multiple paths, increasing the likelihood that it will be received. Each CAP file contains a unique identifier, so the receive device knows if that message has already been received by this device and that it is safe to ignore any copies.

CAP is also a world-wide standard ratified by the Organization for the Advancement of Structured Information Standards (OASIS). As the world continues to shrink, having the ability to share alerts across borders (for distribution by the proper local authorities, of course), improves our ability to communicate clearly when clarity is most critical.

Why CAP?

The benefit of CAP is that the structure enforces rules that can be followed by multiple devices. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems. This ability to concurrently communicate with multiple diverse platforms increases warning effectiveness while simplifying the tasks required to issue an alert. Additionally, these CAP alerts contain more detail about the incident than has been possible to deliver historically.

Because CAP files are digital computer files, when a CAP file comes in, the receiving device can be programmed to take action according to what it finds inside the alert. For example, siren may be programmed to sound if the type of threat is a tornado warning, but not a watch and then only if the certainty is "observed" and the severity is "extreme" or "severe". If all conditions are met, the siren will sound. If any of the conditions are not met, the siren will not sound. Multiply this automatic processing over many devices that currently have to be triggered by hand and you can see how CAP holds the potential to drastically change the way we work.

Many jurisdictions have accumulated multiple ways of distributing both public and private alerts. In addition to triggering EAS, you may have the ability to send text messages, reverse 911 calls, sound sirens, post text to electronic message boards and more. This multi-modal approach to alerting is the key to effective warning. However, as you add systems into a patchwork of manual processes, the complexity of sending alerts skyrockets.

Just keeping track of all the steps can be mindboggling. What button do you push to sound the siren, which has not been used since it was installed? Who has the password to the system that sends out text messages? Where is the microphone you use to record a reverse 911 message and which computer manages the opt-in database? All of that can be

managed in a single CAP alert. Each device receiving the CAP file will take appropriate action based on how it was programmed to respond to the different elements in the file.

Of course, this puts a lot of pressure on the person creating the file to "get it right." CAP system vendors, including SpectraRep, can assist by providing templates that have all of the proper values for certain types of events, allowing the user to control access to certain parts of the CAP file. This can be done based on user authentication, thus allowing remote users with the most knowledge to originate or pass control as needed.

CAP can reduce cost and operational complexity when creating and distributing emergency alerts. This is accomplished by eliminating the need for multiple, and sometimes redundant, interfaces to the many warning devices used today.

CAP benefits include:

- Flexible geographic targeting using County boundaries as well as polygons and circles on a map
- Multilingual and multi-audience messaging
- Phased and delayed effective times and expirations
- Enhanced message update and cancellation features
- Template support to speed alert creation
- Digital encryption and signature capability
- Ability to associate files, graphics, audio and video with the alert

In short, CAP is a universal alerting language that allows originators to send one message, over multiple distribution networks, to the public or targeted groups, enabling appropriate action to be automatically taken by the multiple receive devices.

How does CAP work?

As mentioned earlier, CAP is nothing more than an XML file that contains specific information related to an alert. XML is a way of organizing information in a structured way that computers can easily understand.

XML uses a process called parsing to delineate the separate data elements in the file. Parsing is similar to the process of storing and retrieving data from a database. XML provides rudimentary database-like capabilities, without having all of the overhead a real database requires. Also,

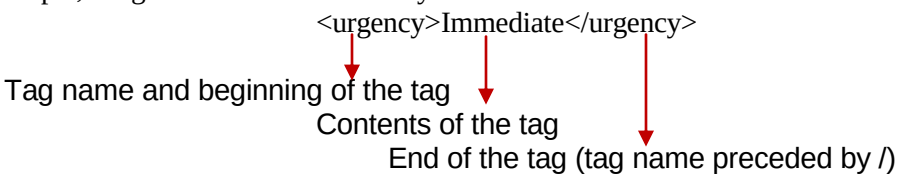
because the data is just ASCII text, it can be opened in any program, even a DOS prompt, so no special software is needed.

XML uses tags to delineate the start and stop points for information that needs to be passed on. Computers can make sense out of 0's and 1's arranged in a certain order, but we humans find that difficult to process. XML is a way to send very specific information to a computer, while also allowing it to be read and understood by a human.

Dissecting CAP

XML uses this basic structure to communicate. The beginning of a specific data element starts with the name of the tag in brackets, followed by the content of that tag, concluding with a "/" and the name of the tag in brackets again.

For example, a tag in a CAP XML file may look like this



In this example, you can see that this tag relates to the urgency of the alert and that the value is "Immediate". The computer in a receive device that has been given the appropriate CAP schema, also knows this and can respond accordingly.

A CAP file is a collection of these instructions strung together into one file that gets delivered to a device that will take action according to how it has been instructed, like this

<urgency>Immediate</urgency> → The urgency of the alert is Immediate
<severity>Extreme</severity> → The severity is Extreme
<certainty>Observed</certainty> → The certainty is Observed
<description>A Tornado has been observed near the corner of Oak and Elm streets. It has already caused minor damage to three houses in that area and is expected to strengthen as it heads south.</description> → The description provides details to explain what is happening

See an example of a complete CAP file in Appendix A.

CAP History

Art Botterell, a nationally recognized expert in emergency communications, came up with the idea of a structured language for emergency alerting in 1999. In 2000, he organized the original open-

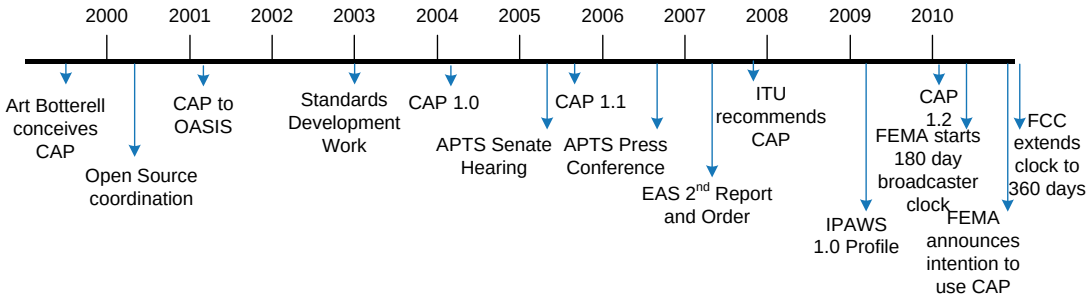
source effort to define it. Art shepherded CAP through a series of trials and revisions over the years. In 2001, he contributed the work to the international standards body the Organization for the Advancement of Structured Information Standards (OASIS). In April 2004, OASIS released version 1.0 of the spec and the alert and warning community started to look at CAP as a way to centralize and organize the disparate alerting options and systems.

Throughout 2004 and 2005, the Association of Public Television Stations (APTS), enlisted SpectraRep, to conduct meetings and CAP alerting demonstrations on Capitol Hill. SpectraRep worked with Washington, DC's public television station, WETA, to deliver demonstration CAP alerts into lawmakers' offices using a small TV antenna. These demonstrations led to a demonstration for the Senate Commerce Committee in July of 2005 at which support for CAP and using the public television infrastructure was endorsed. In October 2005, CAP 1.1 was adopted by OASIS.

In July 2006 APTS held a press conference that included a live over-the-air demonstration using WETA-DT's television signal. FEMA used SpectraRep's AlertManager software to create a CAP message with associated live video and file attachments. That alert was sent to the PBS satellite uplink in Washington, DC, where it was received by public television stations around the country, and seamlessly added to their TV signal. Receivers at WETA and the New Jersey Network (NJN) received the alert, the associated files and live video from FEMA.

As part of the standardization process, the International Telecommunication Union (ITU) recommended CAP in 2007. The FCC also released the EAS second report and order in 2007, mandating that all EAS participants be able to receive a CAP formatted EAS alert no later than 180 days after FEMA publishes the technical standards and requirements. FEMA did just that on September 30, 2010. CAP 1.2 was also adopted in 2010.

The timeline of the history of CAP is shown below:



One benefit of CAP is that it provides for the flexibility to address specific vertical market needs, without changing the base structure. These external "profiles" add capabilities to the core functionality. While all CAP receive devices can process any CAP file, even one with a special profile, only devices programmed for these additional profiles will be able to take advantage of the additional instructions. The first profile adopted was for FEMA's Integrated Public Alert and Warning System (IPAWS) in October 2009. Other profiles for hospitals, other countries and more were added later.

How does CAP improve alerting?

For now, CAP is another input into the EAS Encoder/Decoder (ENDEC) equipment at every radio, television, cable and satellite television operation. Adding CAP inputs can be accomplished by upgrading to a digital EAS decoder, or by adding a small appliance in front of an existing analog ENDEC to process the CAP file and generate backwards compatible Frequency Shift Key (FSK) tones to trigger the legacy device.

However, CAP can do a lot more than just trigger ENDEC's. As mentioned earlier, the power of CAP is the ability to have a single alert message generate appropriate, and perhaps disparate, action in multiple receive devices. The existing EAS system is just the tip of the iceberg.

The headline of a CAP file might be sent to a roadside sign. A siren might sound and then play an attached audio file. RSS feeds, text messages and emails may be automatically generated. All of these actions can take place as appropriate from a single CAP alert sent to all of these devices.

CAP alerts do not even need to be designed for public consumption. Private alerts may be used to keep employees, law enforcement and public safety officials informed. Because CAP can be encrypted and distribution controlled and targeted, CAP can be used to standardize notifications and updates in addition to alerts.

CAP alerts can be targeted much more discretely than the county boundaries EAS uses. Geocoded circles and polygons on a map can be used to send messages only to people inside those boundaries. Since CAP messages can contain associated computer files, we are no longer reliant on a short

audio description of the event. Imagine seeing a picture of the missing child, a video of the tornado, a blueprint for the building on fire. Clearly, the alerts we will send in the future will convey more information, be distributed more efficiently and be more effective in managing emergency events.

The Future – Beyond EAS

The United States emergency community has been using a single thread analog alerting infrastructure since the mid 1960's. CAP is a giant leap forward in capabilities, but it is only part of where we are headed.

In the early days, radio was the only way to reach the general public. Television, and eventually cable television, were added as we grew from fireside chats to a hundred channel universe. How do you incorporate the Internet, social media, cell phones and whatever the future holds?

EBS was originally designed so the president could talk to the American public and inform them as emergency events were unfolding. Neither EBS, nor EAS, was ever activated at the national level. Television stations now fly their own helicopters and the president talks to the American people on national TV news broadcasts. However, relying on third-party infrastructure and assuming that they will be there when the president needs to address the nation is not the way to assure reliable communications during a crisis.

The future of alerting will most likely include a multi-modal approach:

- all broadcast media
- personal media in use now and in the future (cell phones)
- social media
- computer desktops
- interconnected devices (sirens, roadside signs, message displays)

It may be decades into the future before we completely revamp emergency alerting again, but rest assured that the capabilities we are putting in place today will not remain static. CAP is flexible enough to morph as the future presents new opportunities and obstacles. The CAP based alerting system we use years from now is unlikely to look anything like what we are deploying today. The thread that is likely to remain at the heart of all these disparate end points and distribution networks is CAP. Hats off to the protocol that will allow emergency alerting to grow with us and adapt as needs and methodologies change.

Questions and Answers

1. Is EAS going away?
   - No, there is no timeline for phasing out or eliminating the existing EAS system. That could happen in the future, but it is more likely that EAS will evolve into a redundant or backup alert system. For now, EAS remains the primary way of notifying the public, CAP just provides another input into EAS, just like adding another monitoring point. When CAP is used to trigger EAS, those messages will have the same limitations as EAS alerts triggered by traditional methods. CAP provides considerably more features and benefits than EAS, and those benefits will be realized as more receive equipment becomes CAP enabled. The current vision includes direct CAP reception on cell phones, to Internet connected computers, to special radios and more, but EAS will remain as well.

2. What do State and local emergency officials need to do to issue CAP EAS messages that will get to broadcasters?
   - CAP message creation software will need to be acquired. Several companies make this software. The end result is always the same no matter what system is used to create the CAP compliant alert file. However, each company goes about it slightly differently, so several options should be evaluated. Most use some sort of web based access to a server that both creates and sends the message out. Some companies use cloud servers, some use local servers. Distribution can be over the Internet, satellite, or digital television; any IP transport can be incorporated. Most support multiple delivery paths, eliminating the daisy chain and allow for template creation for quick and easy alert creation. SpectraRep uses the Internet, satellite and partners with public broadcasters to use digital television to assure message delivery.

3. What happens when the CAP file is received?
   - CAP compliant software is required at the receive end as well. This software is incorporated into the new digital EAS decoders from all of the manufacturers. CAP processing software is also available in standalone appliances that can interface with legacy EAS decoders. These appliances generate appropriate FSK tones for backwards compatibility with legacy EAS equipment.

4. If the CAP file is sent over multiple delivery paths, what happens when the same file is received multiple times?
   - CAP alerts can be sent simultaneously over multiple paths. This improves resiliency and increases the likelihood that the alert will reach its destination even if some of the paths are blocked. The first one to reach the receiver will trigger it, other copies of the same message will be ignored. Each CAP file contains a unique id in the identifier tag, which identifies that unique file and can be used by the CAP receive software to flag copies.

5. What benefits does CAP provide beyond triggering EAS?
   - In addition to providing more reliable distribution and reducing or eliminating the daisy chain, CAP files contain much more information about the alert than can be sent in audio FSK tones. Dozens of unique data points provide great detail. Unlimited length text descriptions, map based geographic targeting and file

attachments like weather maps, hazardous material information and any other associated data can be sent along with the alert. AMBER alerts can now contain a picture of the missing child, for example. This data can be used outside of EAS to better inform alert recipients, like broadcast newsrooms.

6. How will all this new CAP supported data get to the public?
   - For now, CAP becomes another input into EAS equipment for traditional audio alerting over radio and television. Broadcast newsrooms will receive alert related information in file attachments that can go right to air. Non-EAS devices like sirens, text message systems, roadside signs, etc., will receive the CAP file and respond appropriately.

7. Can legacy EAS equipment that is part of a state operated Local Relay Network be used to issue and receive CAP messages?
   - Legacy EAS equipment is by definition not CAP compliant, so it cannot be used to create or receive CAP alerts without some system updates. Each manufacturer will make their own decision regarding software updates that will allow CAP functionality, but it is most likely that new equipment will need to be purchased or at least new web based origination deployed. On the receive end, this new equipment may be an interstitial device that goes between the legacy equipment and the alert originator, or a new device that supports both CAP and legacy EAS.

8. Does adding a CAP converter in front of legacy EAS equipment comply with the new EAS rules?
   - Yes. CAP compliant processing devices added to legacy equipment will make a broadcaster compliant with the rules. These devices receive the CAP file and associated attachments, then generate backwards compatible FSK tones to trigger legacy existing EAS decoders. Check with each manufacturer for details. Much of the legacy EAS equipment is older and nearing end of life, so it is expected that most stations will buy new CAP compliant EAS devices.

9. Will the converters work with the state requirements, including Governor's activation?
   - Yes. The CAP standard is evolving and new capabilities like Governor's activation are supported now. All manufacturers have allowed for updates as CAP evolves and adds new capabilities. This is usually managed as a software or firmware update. Check with each manufacturer for details.

10. Can State and local officials issue CAP EAS activations through an integrator or CAP service provider? If an integrator is used, do officials need EAS equipment? How will broadcasters receive activations that are sent through an aggregator?
    - Aggregators typically use the Internet to deliver CAP alerts. It may be possible to create CAP files using a web interface over the Internet. This may be a fast and cost effective option for some, or it may be part of a multi-modal strategy that incorporates other delivery paths in the future. Broadcast stations that receive CAP files from integrators will receive them over the Internet. SpectraRep typically uses closed delivery networks like satellite and digital TV, but we use Internet as a failover path as well.

11. Do broadcasters need to have EAS equipment made by the same manufacturer? Does it need to be the same as the EAS equipment used by State or local officials? How do stations decide what to buy?
    - No the manufacturer of the equipment does not matter. One of the benefits of CAP is that it is a standards based protocol that all receive devices understand. It is possible to add elements to a CAP message that are unique to a specific device. This may be especially evident in additional protocols like the IPAWS profile, Canadian profile, etc. However, the elements required to trigger EAS are rigid and must be implemented equally by all manufacturers. FEMA operates a test lab at the University of Kentucky to test CAP and backwards EAS compliance for originate and receive devices. Any device that passes this certification can be used with any other manufacturer's equipment.

12. What if emergency officials decide they don't want, or can't afford, to buy CAP compliant EAS equipment? Can they continue going through the Local Primary Station to originate activations?
    - Yes. The 180 day clock for CAP compatibility started by FEMA on September 30, 2010 only requires that broadcasters install CAP compliant equipment and be able to receive and process national alerts in CAP format. In the near-term, these CAP initiated alerts will be distributed to the public primarily through legacy EAS. Local and state origination can continue to use legacy processes as well, but the benefits of CAP will not be realized until CAP compliant origination equipment is installed.

13. What about counties where officials have been trained to use the NWS HazCollect system — how will information from those activations get into the CAP system?
    - FEMA will be sending CAP alerts over a system that is similar to HazCollect called IPAWS-OPEN (formerly DM-OPEN). EAS decoders at broadcast stations will monitor IPAWS-OPEN and ingest any CAP files posted there. It may be possible for state and local agencies to deliver CAP alerts the same way. It will also be possible to create a similar cloud based CAP alert server for state and local use. Other networks like existing point-to-point microwave, digital television, etc. can also deliver CAP files to a local server that can be monitored over a Local Area Network for ingest when new CAP files arrive.

14. Can a CAP EAS system be easily accessed by all local First Responder agencies—fire departments, professional and volunteer, state and local fire marshals, wildfire agencies, police departments, sheriffs offices, state and local public health officials, utility managers, highway patrol and state troopers?
    - One of the benefits of CAP is that it is not limited to EAS activation. While it is backwards compatible with legacy EAS, private alerting and emergency information distribution are among the possible uses. As long as the recipient has a CAP compliant receive device CAP can be the backbone of these systems. The receiver may be a police radio, a hop on a private microwave system, a digital television receiver or any other device. Even computer desktops running SpectraRep's ActiveAccess software can directly receive CAP files over the Internet or any other network to which it is attached.

Appendix A

Sample CAP File

```
<?xml version="1.0" encoding="UTF-8"?>
<alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.2">
<identifier>9720101027142727</identifier>
<sender>mobrien@spectrarep.com</sender>
<sent>2010-10-27T14:27:27-04:00</sent>
<status>Actual</status>
<msgType>Alert</msgType>
<source>State Police</source>
<scope>Public</scope>
<info>
  <category>Rescue</category>
  <event>Child Abduction Emergency</event>
  <language>en-us</language>
  <responseType>Monitor</responseType>
  <urgency>Immediate</urgency>
  <severity>Severe</severity>
  <certainty>Likely</certainty>
  <audience>All recipients</audience>
  <eventCode>
    <valueName>SAME</valueName>
    <value>CAE</value>
  </eventCode>
  <expires>2010-10-27T23:00:00-04:00</expires>
  <senderName>Mark OBrien</senderName>
  <headline>ACTIVE AMBER Alert TEST: Mary Jones has been reported missing and may have
   been abducted by her father</headline>
  <description>This is an activation of the AMBER Alert System. We have just received this
   important information regarding an abducted child. The state police are looking for a child who
   was last seen near fourth and Main and may be in danger. The child's name is Mary Jones. She
   is believed to be 2ft 3in tall, weighing 34lbs with light brown hair and green eyes. She was last
   seen wearing a red plaid jumper. Authorities say that the child may be in the company of John
   Jones.  He is a 25year old white male with blonde hair and blue eyes. He is believed to be 6ft 3in
   tall, weighing 180lbs. He was last seen wearing a red shirt and jeans. He may be traveling in a
   2010 Blue Dodge Pickup, with license plate:XX123123. If you have any information on the
   whereabouts of this child please call 911 or contact the state police at 123-234-2343
   immediately.</description>
  <instruction>Please Call State Police at 123-234-2343 if you have any information</instruction>
    <resource>
      <resourceDesc>Picture of Missing Child</resourceDesc>
      <mimeType>Image/JPG</mimeType>
      <uri>http://child.jpg</uri>
  </resource>
  <area>
    <areaDesc>District of Columbia, DC</areaDesc>
    <geocode>
      <valueName>SAME</valueName>
      <value>011001</value>
    </geocode>
  </area>
</info>
</alert>
```

References

[1] CTIA Semi-Annual Wireless Industry Survey

a. http://www.ctia.org/blog/index.cfm/2010/10/6/SemiAnnual-Wireless-Industry-Survey-Results-Wireless-Data-Consumer-Value-Continues-to-Grow

Internet References

(1) IPAWS Web site
   a. http://www.fema.gov/emergency/ipaws/
(2) OASIS CAP Standard v1.2
   a. http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html
(3) IPAWS Specification to the CAP Standard (CAP v1.2 IPAWS USA Profile v1.0
   a. http://docs.oasis-open.org/emergency/cap/v1.2/ipaws-profile/v1.0/cap-v1.2-ipaws-profile-v1.0.pdf
(4) CAP-EAS Implementation Guide
   a. http://www.eas-cap.org/ECIG-CAP-to-EAS_Implementation_Guide-V1-0.pdf
(5) FEMA News Release announcing CAP standard for emergency alerts
   a. http://www.fema.gov/news/newsrelease.fema?id=52880
(6) FCC EAS Website
   a. http://www.fcc.gov/pshs/services/eas/
(7) FCC Second Report and Order for EAS
   a. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-109A1.pdf
(8) Presidential Executive Order 13407
   a. http://edocket.access.gpo.gov/2006/pdf/06-5829.pdf
(9) Incident.com CAP Cookbook
   a. http://www.incident.com/cookbook/index.php/Main_Page

About SpectraRep

SpectraRep has been offering creative content distribution services to the public safety community for 11 years. Utilizing excess spectrum from television stations around the country, Spectrarep's technology can deliver incident response files, live video and CAP alerts anywhere they are needed, even during an emergency when other bandwidth options are limited or constrained.

SpectraRep's products include desktop alerting, CAP alerting software and incident response applications that assure Continuity of Operations during emergencies.

Desktop Alerting

- Ties into existing notification systems
- CAP compliant
- Breaks through clutter
- Looks like a TV crawl

Common Alerting Protocol

- New digital alerting standard
- Early prototype for FEMA
- Public and private alerting
- Robust delivery over multiple transport

Incident Response

- Uses digital television signal
- Emergency data to first responders
- Secure, private wireless channel
- Natively multicast

About the Author

Mark O'Brien is a co-founder of SpectraRep. He developed several software applications that bridge broadcaster's ability to deliver information to an unlimited audience with public safety's need for better situational awareness and incident response data. He developed security, targeting and encryption systems to assure secure communication over broadcast television infrastructure. Mr. O'Brien has thirty years of experience in consulting, engineering, finance, sales, broadcast station management and ownership.

SpectraRep
15120 Enterprise Court
Chantilly, VA 20151
703-227-9690
mobrien@spectrarep.com