



---

March 2012  
CAP Implementation

WORKING GROUP 9

Final Report – Part 3 September 2012

## Table of Contents

1 Results in Brief.....	3
1.1 Executive Summary .....	3
1.1.1 Report Format .....	3
2 Introduction .....	4
2.1 CSRIC Structure .....	4
2.2 Working Group 9 Team Members .....	5
3.0 Objective Scope and Methodology.....	6
3.1 Objective .....	6
3.2 Scope .....	6
3.3 Methodology.....	6
3.3.1 Sub-Group Structure .....	6
3.3.2 Collaboration via Portal .....	7
4 Background.....	8
4.1 Emergency Alert System (EAS).....	8
4.1.1 Second Report and Order - Further Notice of Proposed Rulemaking .....	8
4.1.2 Third Further Notice of Proposed Rulemaking.....	8
4.1.3 Fourth Report and Order .....	9
4.1.4 Fifth Report and Order .....	9
5 Analysis Findings and Recommendations .....	11
5.1 Analysis.....	11
5.2 Findings.....	11
5.3 Case Studies.....	12
5.3.1 Case Study: Emergency Alert System for Washington State .....	12
5.3.2 Case Study: Emergency Alert System for Oklahoma .....	14
5.3.3 Case Study: Teton County and CAP EAS Case Study.....	17
5.3.4 Michigan EAS Case Study – August 2012.....	21
6 Recommendations/Best Practice Guidelines .....	27
6.1 Best Practice for Message Origination .....	27
6.2 CAP Message Preparation .....	27
6.2.1 EAS and CAP Audio.....	27
7 Mandatory CAP Message Checklist.....	28
8 Optional CAP Message Checklist.....	29

9 Best Practices.....	31
9.1 Best Practice for “Text to Speech” .....	31
9.1.1 Message Originators .....	31
9.1.2 Alert Messages.....	31
9.1.3 Entry of Address or Extensions.....	31
9.1.4 Reference Guidelines.....	31
9.2 Best Practice for Audio .....	31
9.3 Best Practice for SSL Certificates.....	33
9.3.1 Common Root Certificates .....	33
Appendix - EAS Style Guide.....	34
Appendix References .....	35

This space left intentionally blank

# 1 Results in Brief

## 1.1 Executive Summary

The Emergency Alert System is the primary warning system that provides the President with the means to address the nation during a national crisis. Over the years it has gone through several transformations but until recently can best be described as an analog delivery system.

On May 31, 2007, the FCC adopted a Second Report & Order to strengthen the development of next generation technology for the Emergency Alert System (EAS)<sup>1</sup>. This R&O requires EAS participants to accept messages using Common Alerting Protocol (CAP) digital delivery.

Subsequently, on November 18, 2010 the FCC adopted the Fourth Report & Order to establish the deadline for EAS participants to start receiving CAP messages no later than June 30, 2012<sup>2</sup>.

On January 10, 2012 the FCC released the Fifth Report and Order which further clarified the process to receive and transmit CAP messages for the EAS and to streamline the Part 11 rules<sup>3</sup>.

CSRIC Working Group 9 was established to provide recommendations and best practice for the deployment of CAP and to provide an overall progress report on the first months of CAP implementation.

### 1.1.1 Report Format

The first part of our report covers State and Local Government use of CAP EAS. State and local governments have made great strides in implementation of CAP alerting. The Working Group reviewed four distinct case studies of state and local CAP architectures, representing a diversity of technical approaches, using different background technologies.

These case studies provide good insight into challenges faced by early adopters of CAP and demonstrates the need to provide new standards and best practices for all CAP implementation.

The second part of our report describes best practices being used in real world application of CAP EAS. The following Best Practices will be submitted.

- 1.1.1      Best Practice for Message Origination
- 1.1.2      Best Practice for “Text to Speech”
- 1.1.3      Best Practice for Audio
- 1.1.4      Best Practice for SSL Certificates

Finally we will be presenting a “Style Guide for CAP Origination.” We feel this is important to ensure message dissemination is done consistently across the many operational units.

---

<sup>1</sup> FCC Second Report and Order, in the Matter of the Review of the Emergency Alert System, EB Docket No. 04-296, Adopted: May 31, 2007

<sup>2</sup> FCC Fourth Report and Order, in the Matter of the Review of the Emergency Alert System, EB Docket No. 04-296, Adopted: September 15, 2011

<sup>3</sup> FCC Fifth Report and Order, in the Matter of the Review of the Emergency Alert System, EB Docket No. 04-296, Adopted: January 9, 2012

## 2 Introduction

CSRIC was established as a federal advisory committee designed to provide recommendations to the Commission regarding best practices and actions the Commission may take to ensure:

- Optimal operability
  - Security
  - Reliability
  - Resiliency of communications systems
- Including:
- Telecommunications
  - Media
  - Public safety communications systems

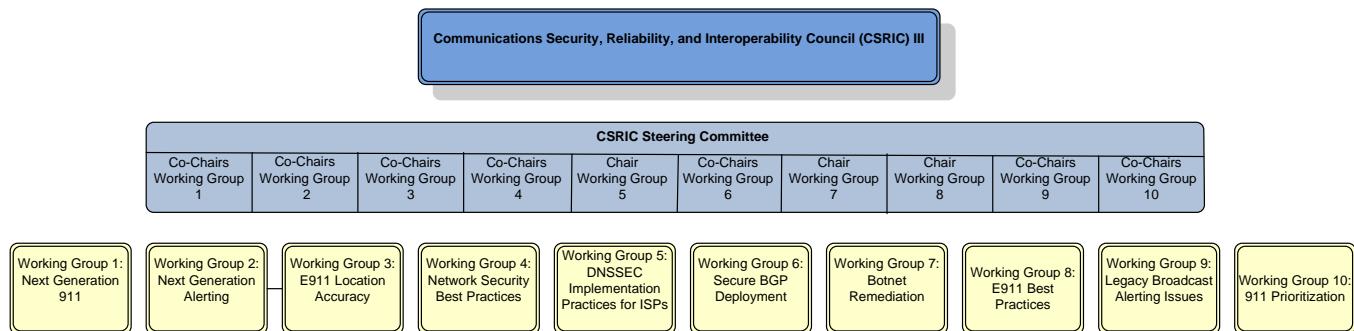
Due to the large scope of the CSRIC mandate, the committee then divided into a set of Working Groups, each of which was designed to address individual issue areas. In total, 10 different Working Groups were created, including Working Group 9 on EAS CAP Implementation.

Working Group 9 officially started its work in December 2011 and was given until March 2012 to produce this First Report. The focus for Working Group 9 is to:

- Review the Fifth R&O (released January 10, 2012) on CAP deployment
- Provide FCC recommendations for best practices to facilitate CAP implementation on national, state and local levels
- Identify technological challenges.

The second report, due in December 2012, will review the progress of CAP implementation by EAS Participants for both national and state level.

### 2.1 CSRIC Structure



**Figure 1 - CSRIC Structure**

## 2.2 Working Group 9 Team Members

Working Group 9 consists of the following members:

Name	Company
Al Kenyon	Federal Emergency Management Agency (FEMA)
Andy Scott	NCTA
Arthur Leisey	EAS Consultant
Bill Marriott	Comlabs
Bill Robertson	Digital Alert Systems (Monroe Electronics, Inc.)
Bob Sherry	Intrado
Chris Homer (Chair)	DIRECTV
Clay Freinwald	Washington SECC
Daryl Parker	TFT
Donald Walker	GRM
Edward Czarnecki (Co-Chair)	Monroe Electronics, Inc.
Doug Semon	Time Warner
Gary Timm	Wisconsin SECC
Harold Price	Sage Alerting Systems
Jeb Benedict	CenturyLink
Jeff Staigh	Univision
Jim Gorman	Gorman-Redlich
Kelly Williams	National Association of Broadcasters
Larry Estlack	Michigan Association of Broadcasters
Matthew Straeb	GSS
Michael Hooker	T Mobile
Mike Nawrocki	Verizon
Ron Boyer	Boyer Broadband
Tim Dunn	T Mobile
Eric Ehrenreich	FCC Liaison

Table 1 - List of Working Group Numbers

## 3.0 Objective Scope and Methodology

### 3.1 Objective

In its January 2012 EAS Fifth Report and Order (EB Docket No. 04-296), the Commission sought to continue the process to transform the Emergency Alert System (EAS) into a more technologically advanced alerting system by revising Part 11 Emergency Alert System (rules) to specify the manner in which EAS Participants must be able to receive alert messages formatted in the Common Alerting Protocol (CAP) and streamlining Part 11 rules to enhance their effectiveness and provide clarity.

The Fifth Report and Order is the second of two orders that implement Part 11 rule changes stemming from the Third Further Notice of Proposed Rule Making (FNPRM). The previous order, Fourth Report and Order, addresses the single issue of establishing a new deadline of June 30, 2012 for meeting the various CAP-related requirements that the Fifth R&O codifies. The Working Group was asked to review the new order to provide insight, implementation recommendations and status. In this Fifth R&O Report, the Working Group shall also recommend actions the FCC could take to improve EAS as it incorporates the new CAP protocol.

### 3.2 Scope

Per the Working Group 9 charter, the group found it essential to begin with an initial focus on the FCC Part 11 Rules governing the EAS as it involves best practices to facilitate CAP implementation leading up to and beyond the June 30, 2012 deadline. The committee will be working with real-time data and events as they unfold during the roll out. Based on results of these events the group will gain valuable insight and metrics that will be used for future planning and rulemaking.

### 3.3 Methodology

The Working Group 9 uses a collaborative, inclusive approach to its work. Given the array of expertise, the WG-9 members brought to bear on this effort, it is critical to provide a multitude of forums and mediums through which participants could express their opinions and help shape this Final Report. The following section details the methodology through which WG-9 achieved this objective.

#### 3.3.1 Sub-Group Structure

After its initial set of meetings, the Chair and Co-Chair of Working Group 9 decided to review the structure of the Working Group and develop a plan that would allow for WG-9 to proceed with its study in an organized fashion which leveraged the diverse backgrounds of the Group's membership.

As such, WG-9 broke into two Sub-Groups; WG-9-1 is focusing on National implementation and best practices of CAP, WG 9-2 focusing on the progress of CAP implementation and best practices at the state and local level. The two Sub-Groups have moved forward with independent conference calls that focused almost exclusively on the portions of the CAP implementation most applicable to their expertise.

Each Sub-Group had a Lead who developed an agenda and framed conversation and discussion amongst the participants. On some of the more divisive issues, the Lead worked to bring members closer to consensus and encouraged open dialogue designed to find common ground.

### 3.3.2 Collaboration via Portal

In addition to the regular conference calls, an online collaboration portal was designed and implemented for use by the WG-9 participants. The portal is accessible to all Working Group members throughout the duration of their work on behalf of the CSRIC. Table 2 details some of the most prominent capabilities featured on the Portal and how they were used by the members of the Working Group 9.

Portal Capability	Description of Use
Document Repository	Collaboration space where members posted, reviewed, and edited documents
Forum	Open space where issues were discussed amongst members
Calendar	Central location where all relevant meetings and events were documented

**Table 2**

From its inception, the portal became a useful tool for the Working Group as they shared ideas, resources, and collaborated on common documents, including this Final Report. Given the disparate locations from which the WG-9 members originated, having an online collaboration tool was instrumental to the successful completion of the Working Group's final product.

This space left intentionally blank

## 4 Background

From the onset of WG-9's work, close attention was paid to researching relevant topics, including the EAS, the Integrated Public Alerts and Warning System (IPAWS), the CAP, and the Commercial Mobile Alert System (CMAS) and other alerting methodologies. Several members of the 9 Working Group brought specialized expertise in one or more of these areas and is also members of WG-2 that is focused on future developments in EAS systems.

### 4.1 Emergency Alert System (EAS)

EAS is the primary national warning system that provides the President with the means to address the nation during a national crisis. State and local officials also use EAS to originate warning messages about imminent or ongoing hazards in specific regions. Several Federal agencies share responsibility for EAS at the national level:

- FCC
- FEMA
- National Oceanic and Atmospheric Administration's (NOAA)
- National Weather Service (NWS)

Functionally, EAS is a hierarchical alert message distribution system. Initiating an EAS message, whether at the national, state, or local level, requires the message originator (e.g. FEMA, which initiates EAS alerts at the national level on behalf of the President) to deliver specially-encoded messages to a broadcast station-based transmission network that, in turn, delivers the messages to individual broadcasters, cable operators, and other EAS Participants.

EAS Participants maintain special encoding and decoding equipment that can receive the message for retransmission to other EAS Participants and to end users (broadcast listeners, cable and other service subscribers).

#### 4.1.1 Second Report and Order - Further Notice of Proposed Rulemaking

On May 31, 2007 the FCC adopted a Second Report and Order and Further Notice of Proposed Rulemaking (EB Docket 04-296, FCC-07-109A1) (Erratum, DA-07-4002A1) to strengthen the EAS and to promote the development of fully digital next generation technologies and delivery systems for EAS. The Second Report and Order requires EAS participants to accept messages formatted using CAP, the groundwork for next generation EAS delivery systems, no later than 180 days after FEMA announces its adoption of standards in each case. CAP is intended to ensure the efficient and rapid transmission of EAS alerts to the public in a variety of formats (e.g. text, audio and video) and via different channels (e.g. broadcast, cable, satellite, and other networks).

#### 4.1.2 Third Further Notice of Proposed Rulemaking

On May 25, 2011, the FCC adopted the Third Further Notice of Proposed Rulemaking, in which they sought comment on a wide range of tentative conclusions and proposed revisions to the Part 11 rules that would more fully delineate and integrate into the Part 11 rules the CAP-related mandates adopted in the Second Report and Order. The Commission received 30 comments and 12 reply comments in response to the Third FNPRM.

#### **4.1.3 Fourth Report and Order**

Subsequently, on November 18, 2010, the FCC adopted the Fourth Report and Order in this docket, in which they amended section §11.56 of the EAS rules to require EAS Participants to be able to receive CAP formatted EAS alerts no later than June 30, 2012.

#### **4.1.4 Fifth Report and Order**

Finally, in the January 2012 FCC Fifth Report and Order on EAS (EB Docket No. 04-296), the Commission sought to continue the process to transform the Emergency Alert System (EAS) into a more technologically advanced alerting system by revising Part 11 Emergency Alert System (rules) to specify the manner in which EAS Participants must be able to receive alert messages formatted in the Common Alerting Protocol (CAP) and to streamline Part 11 rules to enhance their effectiveness and to provide clarity.

This space left intentionally blank

## 5 Analysis Findings and Recommendations

### 5.1 Analysis

CSRIC WG9 is examining a broad range of questions relating to the usage of CAP for next-generation EAS;

#### CAP Distribution

1. What CAP-EAS Distribution Network architectures exist at the federal, state and local level?
2. What are the physical and data components of these systems?
3. What are the interface requirements?

#### EAS Network Requirements

1. What is sufficient capacity to relay messages?
2. What availability is required to maintain service?
3. How does authentication work?
4. How is data security maintained? Data accuracy?

### 5.2 Findings

#### **State and Local EAS CAP Implementation**

State and local governments have made great strides in implementation of CAP alerting. The Working Group reviewed four distinct case studies of state and local CAP architectures, representing a diversity of technical approaches, using different background technologies.

There have also been a variety of approaches used for implementation. Some state and local governments have taken a top down approach (Washington State) while others have taken more of a grass roots approach (Michigan).

#### **Distribution Network Architectures**

There was also distinct difference in CAP EAS distribution network architectures – with some systems relying on internet dissemination, others relying on satellite dissemination, and another system using satellite and Internet in tandem.

#### **Architectural Differences**

There are additional architectural differences, with several of these systems being “hosted” or an “application service provider” model, while another is more of a network-centric server or device based solution, while yet another appears as somewhat of a hybrid of the two models.

### Additional Differences

We observed additional differences in approaches to authentication and security among these case studies. While one system may rely on usage of the IPAWS digital signature credentialing for their own message authentication, another may incorporate both end-to-end encryption and authentication measures, while another may rely on simple posting of CAP messages on a webpage or RSS feed. While all four case studies cite interoperability with the FEMA IPAWS system, utilization of IPAWS by these different systems range from reference to the FEMA system as a redundant backup path, to reliance on IPAWS as a primary means of dissemination.

### Early Adoption

Finally, early adoption was a key challenge for many states. Also funding and support may be scarce and there may not be enough trained individuals to provide operations and technical support. Much needed training to get operation personnel up to speed on new systems will need to occur and best practices need to be established.

### Case Studies

These four case studies below represent a geographic and technical diversity. Each case study uses a different set of underlying vendor technologies, budgetary parameters, and operational requirements. The particulars of the vendors and their products have been omitted for the purposes of this report.

## 5.3 Case Studies

### 5.3.1 Case Study: Emergency Alert System for Washington State

Since 1995 and before 2006 the analog Emergency Alert System, (EAS), for Washington State used 11 radio sites and was plagued by poor performance. In 2005, in conjunction with the Federal Emergency Management Association (FEMA), Washington State became one of the first to deploy a state wide CAP EAS delivery system. Funding from FEMA helped create a “proof of concept” pilot for state wide distribution of CAP EAS.

#### Deployment of Single CAP Decoder

One of the first steps was to deploy a single CAP Decoder at the State Emergency Operations Center (EOC) to receive the CAP alert and relay it over the 11 radio stations to broadcasters. The system provides CAP EAS Alert origination by the state EOC and by all 39 counties. In 2005-2006, OASIS CAP protocol 1.1 was adopted internationally, which became the standard used in the state. The CAP network expanded to 27 stations in 2007. The network went statewide to all Primary Stations and state funded radio stations with special funding provided by Washington State in 2010. One of the “key” challenges for the deployment was being an early adopter.

#### Expansion of Radio and Television CAP Alerts

The network has since been expanded to most radio and television broadcasters and CAP alerts can now be generated in all 39 counties by more than 800 Emergency Management designees that are authorized to send EAS alerts. In addition the system is providing alerts to over 120

broadcasters which poll the system every two minutes. By June 30 all broadcasters will also be monitoring IPAWS ATOM feed for national alerts.

There were many initial challenges in developing the system for Washington State as many parts of the system were in early development. Their system is now used as the primary means to deliver with the old analog system used as backup. In addition to improved audio quality the system is more reliable and resilient.

### **Transcoding Files to a Common Format**

The EOC currently has dual MPLS paths to their content aggregator with additional bandwidth available on satellite or wireless as backup. By transcoding various audio files to a common format the system delivers the desired MP3 file format to both IPAWS and broadcasters regardless of input. Any file that is changed or marked invalid by the system will fail the message and send a "failed" state to originator. Transport layer security and authentication is accomplished through Secure Socket Layer (SSL) version 3 security protocol.

### **Connectivity**

The receive party should have an internet connection of a minimum 1 Mb/s bandwidth. It is also recommended that there is redundancy in this connection to provide better system resiliency. Since most broadcasters require internet connections for administrative purposes, email, monitoring and control, then this requirement should not be a tremendous burden. Many broadcasters maintain not only redundancy but some form of diversity which could include using two separate providers in the event one of the providers would lose connectivity.

The acceptance level of this CAP based system has been very high from all parties.

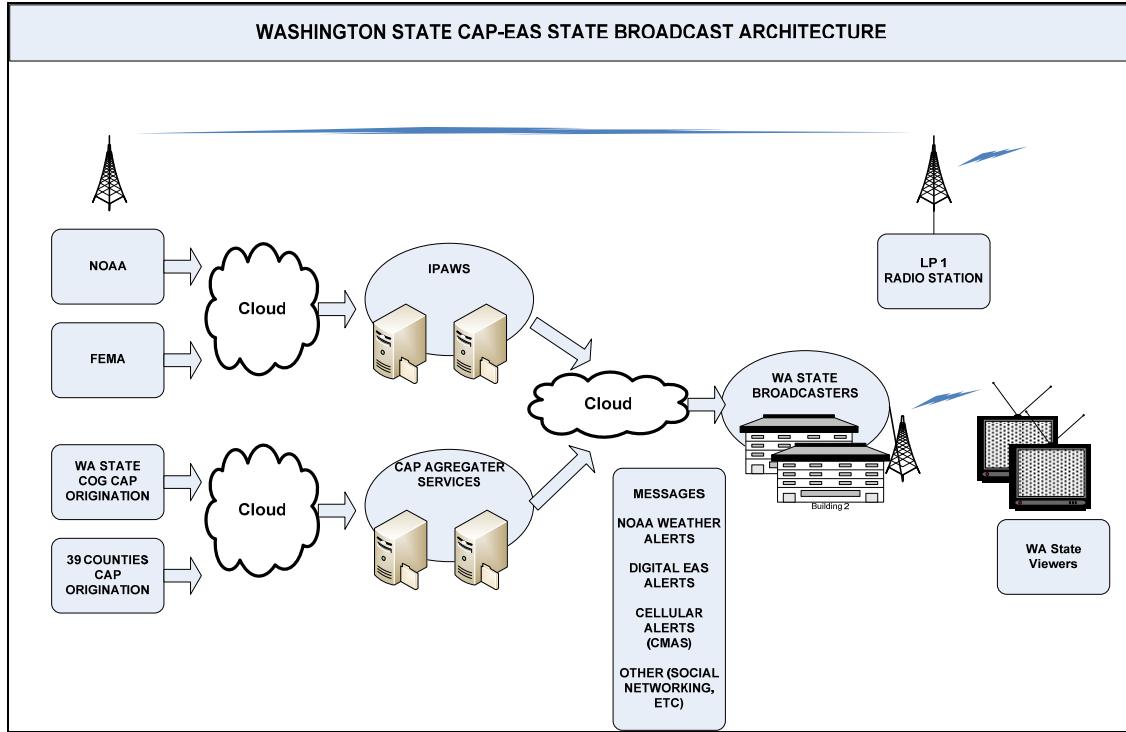


Figure 2

### 5.3.2 Case Study: Emergency Alert System for Oklahoma

The Oklahoma Department of Emergency Management (OEM) started the process of upgrading our Emergency Alert System in early 2011. The primary reason to upgrade the legacy “daisy chain” system was to provide redundancy. The previous system used a VHF transmitter to relay alerts to primary (LP1) radio stations in Oklahoma City. These alerts were then rebroadcast over a variety of systems, some satellite, to secondary (LP2) radio stations, cable, and TV.

The LP2 stations would then rebroadcast the alert to the remaining tiers (tertiary, etc.). The Oklahoma Department of Public Safety (DPS) is also an alert originator and holds primary authority for AMBER alerts; DPS has a dedicated phone line connection to the primary station in Oklahoma City. Another component to this was the FCC’s requirement that all radio stations procure CAP compliant alerting systems.

#### Objectives for System Upgrade

There were three objectives for upgrading the system:

1. Reaching all LP1 stations directly.
2. Allowing for alert origination almost anywhere, the old system required being at the EAS Vendor to originate an alert.
3. Send CAP 1.2 compatible alerts.

The system upgrade was a collaborative undertaking by the Oklahoma Association of Broadcasters (OAB), DPS, and OEM. All three entities met on a regular basis and developed a

strategy to design and implement a solution. OEM offered to fund the installation and maintenance of the system for all entities. As such, OEM is required by governmental purchasing guidelines to complete certain steps, especially for a project of this size. A request for bids (RFB) and contract awarded.

### Contract Details

The contract called for the installation of 16 satellite downlinks and two satellite uplinks. Two of the satellite downlinks and the two uplinks were to be installed at OEM and DPS, respectively. The uplink was to allow for alert origination should internet facilities be offline. The 14 satellite downlinks were installed at designated LP1 stations across Oklahoma.

The alert origination tool is a website, which uses Microsoft's Silverlight<sup>TM</sup>. Downlink installations were completed by a 3rd party vendor and uplink stations by another vendor. Installation took approximately one month, accounting for Thanksgiving. Training on the downlink system was provided by the contractor upon installation. There was little training on the uplink system. The technology provider included web based on training on their simple and useful alert origination tool.

### System Testing

The system is tested weekly using the "Required Weekly Test" alert, which is logged by LP1, OEM, and EAS Decoder units. OAB was initially concerned that the legacy system would be abandoned in-favor of only issuing alerts via the new digital satellite delivered emergency alert system. Oklahoma's EAS plan does outline alert issuance via the legacy system. As such, a cooperative agreement was reached to use the technology provider CAP alert originator to issue alerts and OEM's or DPS's digital emergency alert CAP EAS encoder units would be configured to rebroadcast the alerts using the legacy system. This would prevent duplicate alerts from traversing the system. Minor upgrades to the legacy system are ongoing and this plan will be implemented once completed.

### Actual Use

The system has not been used for an actual event (AMBER, Required Monthly Test, or other emergency). However, the RWT's have been proven successful, with positive feedback from LP1 stations. The two primary drawbacks are:

1. The use of Silverlight for web design this prevents using iPhone<sup>®</sup>, iPad<sup>®</sup> or other non-Microsoft (Firefox<sup>®</sup>) does work systems.
2. Allowing for alert origination almost anywhere, the old system required being at the EAS Vendor to originate an alert.

The satellite uplink installation at DPS and OEM is permanent.

Note: On second thought, a mobile satellite system may have proven a better (potentially less expensive) choice.

#### **Cost**

The new digital emergency alert system does require a reoccurring monthly charge. OEM is handling this expenditure and will continue to do so for the long-term. This project represents the best in public-private cooperation and intends to provide future compatibility for upcoming alerting systems (CMAS, etc).

Figure 3 on the next page illustrates the Oklahoma CAP-EAS Broadcast Architecture.

This section left intentionally blank

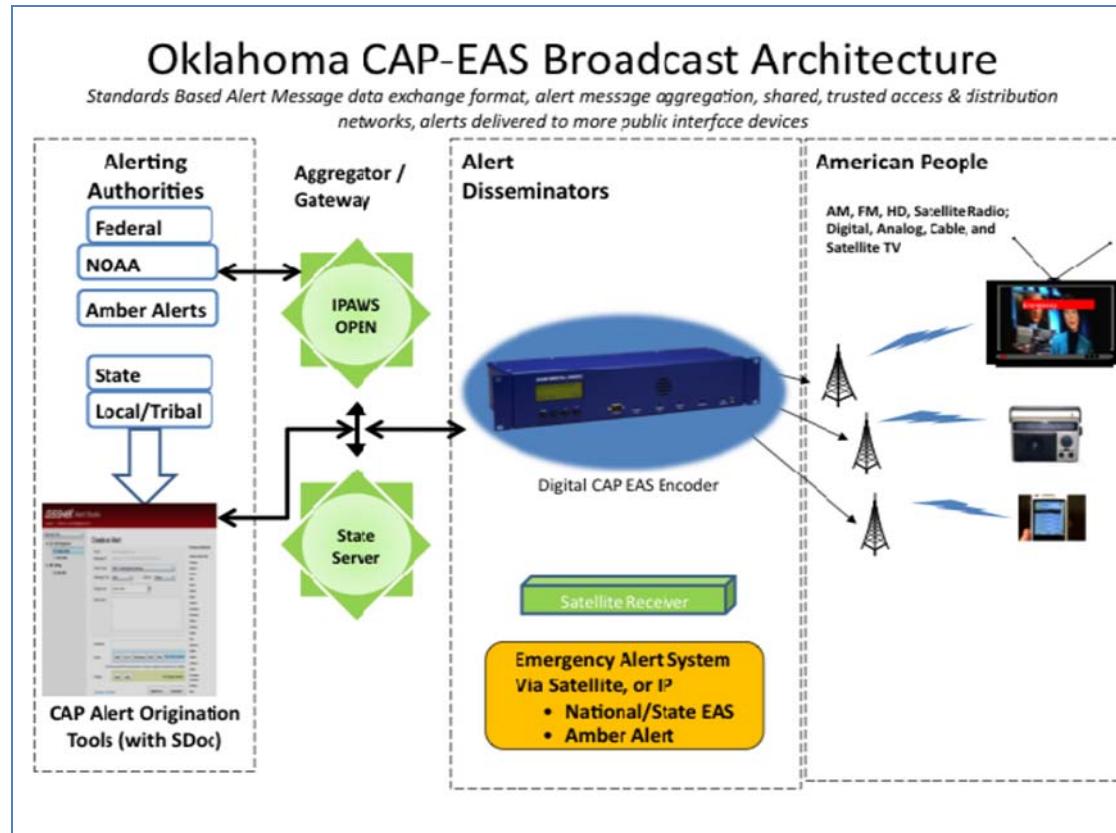


Figure 3

### 5.3.3 Case Study: Teton County and CAP EAS Case Study

Teton County Wyoming Emergency Management (TCEM) has access and authority to activate EAS along with several other key groups. Teton County Emergency Management coordinates the various methods used to alert and immediately inform the public during an emergency situation. These methods are all part of our local area Emergency Alert System (EAS).

#### Conventional EAS

TCEM currently maintains several local systems, including EAS, that are used to alert the public, and also access parts of the state EAS to distribute messages as the situation dictates. Hazards that affect Teton County (in no particular order) are:

- Earthquakes
- Avalanches
- Wildfire
- Severe weather
- Landslides,
- Flooding
- Flash-flooding,
- AMBER alerts
- Any number of man-made disasters

## Teton County Emergency Alert System

As seen in Figure 4, TCEM conventional notification systems give access to several methods of communication during a disaster. At the federal level, the National Weather Service (NWS) can send messages over NOAA All-Hazards Weather Radio network. With one press of the button from the NWS office in Riverton, they can send messages out to all NOAA All-Hazards Weather Radios (which, with the alert function, will turn on automatically), local television, and local radio. Additionally, these messages will be broadcast over Wyoming's law enforcement teletype network, delivering the message to dispatch centers all over the affected area.

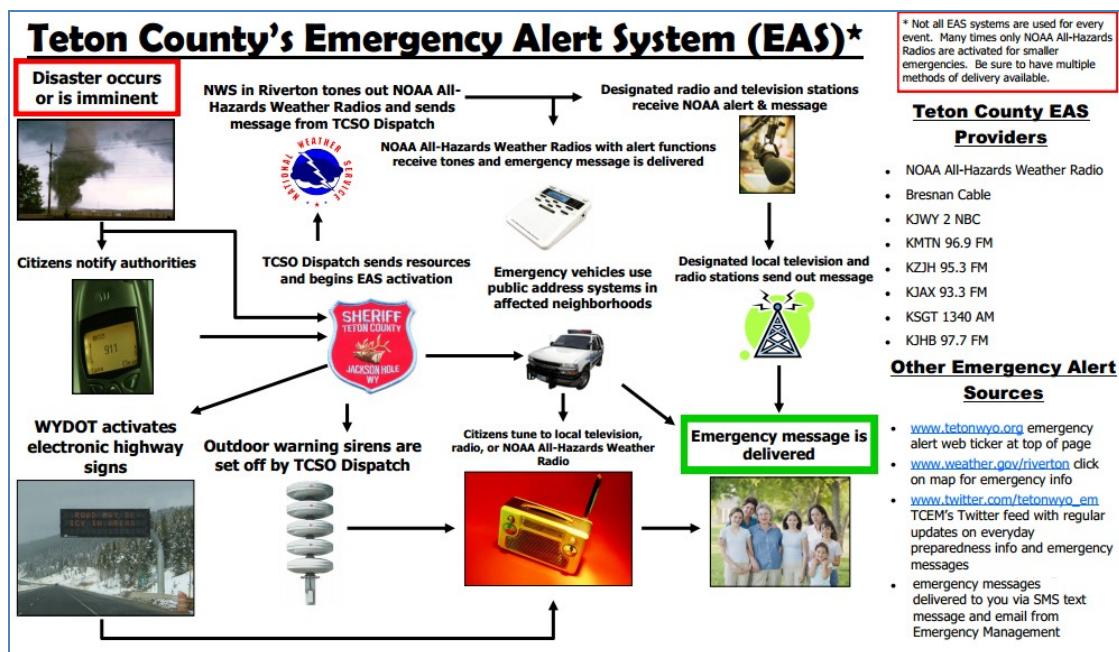


Figure 4

## Local Media Outlet Participation

There are several local media outlets that participate in EAS. They include:

- Bresnan Communications (local cable TV provider)
- KJWY-TV
- Radio stations:
  - FM 95.3 KZJH
  - FM 96.9 KMTN
  - FM 93.3 KJAX
  - FM 97.7 KJHB LP
  - AM 1340 KSGT

Each of these operations currently monitor both the conventional EAS, and will be monitoring the new CAP-based IPAWS system.

### Teton County's Next Generation CAP/EAS Strategy

Teton County Wyoming has implemented a powerful and cost-effective strategy for integrated CAP and EAS capabilities. Teton County has been using an advanced CAP EAS encoder/decoder for conventional EAS activation for several years. This system was recently software upgraded to support integrated simultaneous EAS+CAP+IPAWS origination from a single platform. The upgraded CAP EAS solution posts the CAP message to IPAWS for broadcast (EAS) and mobile phone (CMAS) distribution. The system simultaneously issues legacy EAS transmission via AM/FM radio and broadcast TV.

This single EAS encoder/CAP server combo provides Teton County with the multiple capabilities in one platform:

- Originate CAP for IPAWS
- Originate CAP for local feeds
- Simultaneously originate conventional EAS via broadcast relay
- Monitor inbound alerts from both EAS and multiple CAP sources (for example, IPAWS)

### Monitoring Inbound Alerts

TCEM has found that monitoring inbound alerts is a tremendously useful tool even if they are not forwarded to downstream broadcasters. The fact that TCEM monitors whether LP1 or Primary Nationals are performing their tests as they should, and, if they are correctly relaying alerts from the LP-1 or NOAA, it is a great way to make sure the local EAS is in good working order. A date/time stamped email and record on the CAP EAS unit allows troubleshooting problems or confirms they are correctly putting out tests and alerts.

### FEMA IPAWS CAP Conformity Testing

The decision to undertake this upgrade was based on the equipment's completion of FEMA's IPAWS CAP conformity testing, which was viewed as a key requirement, since the initial plans are to rely on the IPAWS system for CAP message distribution alongside the conventional EAS broadcast relay.

The new system provides CAP and EAS origination from one simple interface. This one device serves as an EAS encoder/decoder and county-level CAP server to manage simultaneous messaging to both the IPAWS Federal server, as well as the local conventional EAS relay.

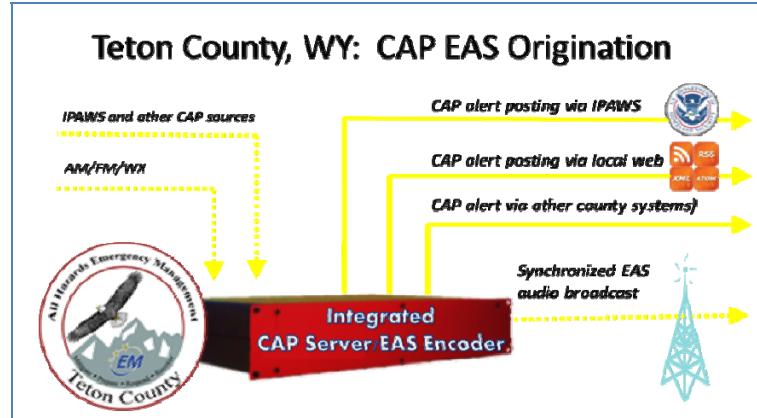


Figure 5

### Teton County and IPAWS

In July 2012, Teton County initiated its first live CAP messages into the IPAWS operational environment, successfully activating all radio, television and cable sites monitoring the IPAWS aggregator in our area. Alert messages were sent as CAP XML text to IPAWS, simultaneously with EAS with text-to-speech or live voice generated at our Emergency Operations Center (EOC).

Local broadcasters and cable operators in the area can now receive our emergency alerts both via IPAWS and the conventional EAS system in a coordinated manner. When alerts are issued, the new CAP EAS system automatically emails all local EAS stakeholders, such as radio station managers, TV managers, cable providers, etc. Mobile phone carriers will also be able to relay urgent messages via IPAWS and Wireless Emergency Alerts.

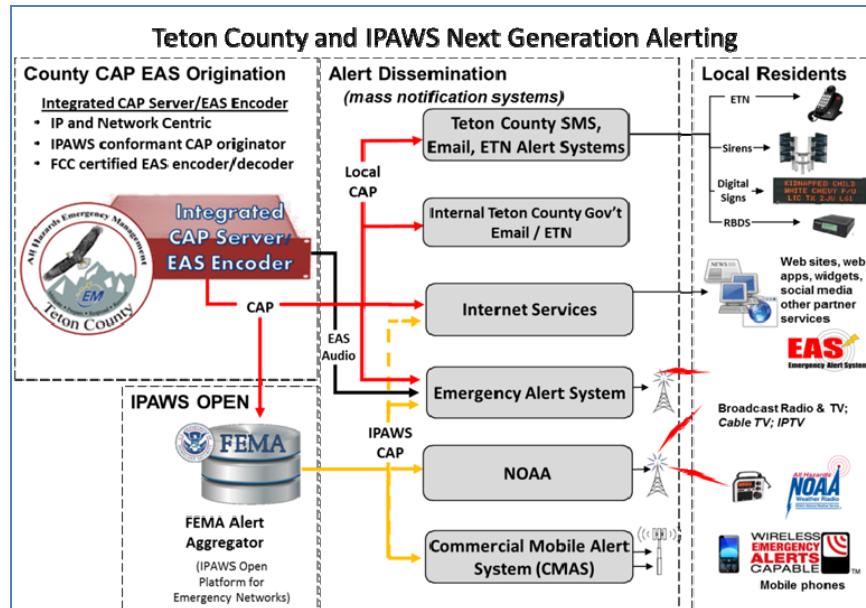


Figure 6

### Risk of CAP and EAS Message Duplication

An additional major consideration was eliminating any possibility that the CAP message may differ from the EAS message. Specifically, TCEM wanted to ensure when CAP and EAS message were issued, duplicate detection was ensured across these two very different message types. The upgraded platform is unique in its ability to eliminate the risk of message duplication. The system produces alert message with the same headers via both CAP (XML) and EAS (audio), this prevents duplicate EAS messages over separate systems being monitored. This is a critical feature for the proper operation of EAS on both the origination and monitoring side.

### EAS CAP IPAWS Capability

While TCEM uses numerous notification systems that are hosted or “virtual,” it is important to maintain this key EAS CAP IPAWS capability within the network, under TCEM control. Additionally, this integrated solution costs significantly less than separate systems for CAP, EAS and IPAWS – both sending and monitoring.

### Next Steps

Future plans include establishing a local ATOM web feed hosted by Teton County to provide authenticated CAP messages. This will provide a local redundant source for CAP messages using the same digital signature authentication provided by the IPAWS aggregator.

In addition, TCEM will seek near-term integration of its CAP EAS originator with other emergency communications systems.

#### 5.3.4 Michigan EAS Case Study – August 2012

In 2008-09, the Michigan Emergency Management Network began to be implemented as numerous counties in several Michigan State Police Districts chose to purchase equipment for each of their counties. Key attributes of the system were its dual path capability (satellite as well as internet), message encryption, full system monitoring and extensive documentation of system activity. These attributes were considered necessary to create a truly flexible, robust and secure system. The system is now used by the State of Michigan, as well. This Michigan case study represents a system architecture that is shared among approximately 18 other states.

### Completed Installations of CAP Compliant Equipment

All broadcast stations and cable systems in the state have also completed installations using new CAP compliant equipment connected to the internet and polling the FEMA server. Thus, multiple paths for emergency communications assure that Michigan residents are informed, no matter what kind of media devices they are using. This system significantly enhanced the capability to provide statewide and local warning and increased information sharing between public safety officials and the general public.

The state CAP network is now installed in every LP 1 and LP 2 station in the state, at the Michigan State Police MIOC and Emergency Operations Centers, plus all counties in the most populated areas in Michigan (Detroit, Grand Rapids and Flint-Saginaw-Bay City), as well as, numerous other MI counties. Emergency alerts can be activated by the Michigan State Police or County Emergency Management officials. It may be requested by municipal authorities to their respective county for activation by the county, if it so wishes.

The system offers a back-bone which can activate many other warning and communications systems with one entry. It allows emergency managers to place important emergency messages on radio and TV, based on mutually agreed upon criteria, even when the station is automated with no one on duty.

### **Michigan State CAP Network and IPAWS**

With the state system's interoperability with IPAWS, qualified alerts will not only be relayed directly to Michigan's broadcasters via Satellite and internet connection. Michigan's link to IPAWS will simultaneously allow broadcasters to monitor these alerts via the IPAWS OPEN web feed, as well as, insert these messages into NOAA Weather Radio. Finally, interoperability with IPAWS will enable transmission of qualified alerts to mobile phone handsets via the IPAWS CMAS system (also referred to as Wireless Emergency Alerts or "WEA").

### **Analog System**

Figure 7 illustrates that Michigan has not forgotten its legacy distribution system, which continues to provide a full analog path as required for federal level messages. Such messages enter the State via the Michigan PEP station, as well as, via the NPR satellite analog audio feed received at the State Primary Station, and a number of additional NPR affiliate stations. Thus, a combination of off-air, satellite and internet streaming carries federal level messages "live"- into Michigan's 83 counties.

### **Digital System**

Meanwhile, in tandem, the digital path operates in a CAP compliant manner, allowing warnings of a State or local level to be transported to all nodes in the state CAP network, as well as, to an aggregation server (on-line fall 2012). This server will provide access to the state CAP network by all CAP compliant devices at broadcast and cable facilities, electronic signage and other future users.

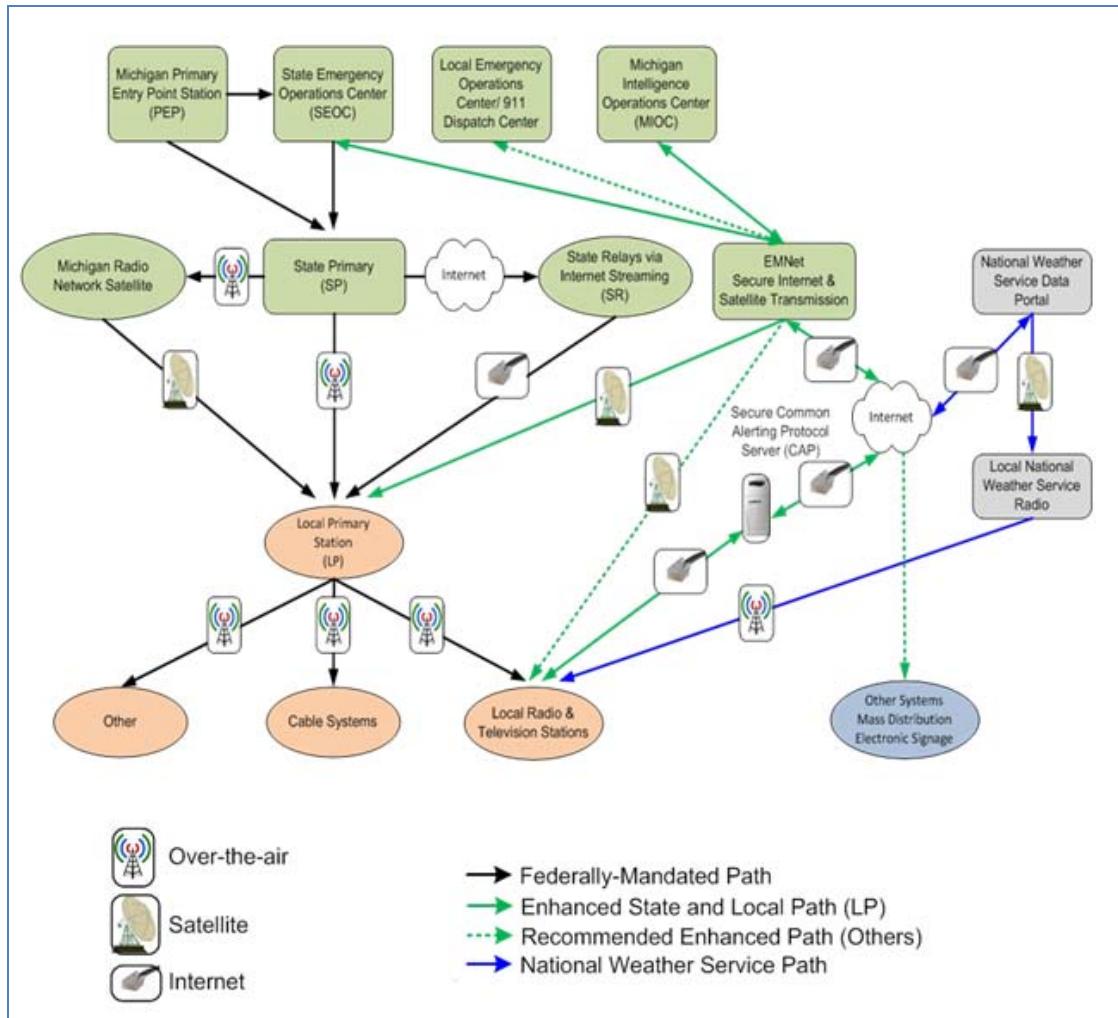


Figure 7

### EAS Warnings in Michigan

On average, Michigan has seen approximately 45 locally originated EAS alerts per year, principally originated at the county level. Of these approximately 30 are AMBER alerts (child abduction). The largest use of EAS overall in Michigan has been for weather alerts, primarily Tornado and Severe Thunderstorm Warnings. In most areas, this process is very successful and fast. In one instance, a Tornado Warning, issued by the NWS in 2010, was monitored on ALL local stations in the EAS area in less than one minute. AMBER alerts are also carried as EAS events and reach the LPs stations seconds after issuance.

### Fully Complaint CAP Broadcast Stations

In 2011, Michigan began the process of outfitting each Michigan broadcast TV station with fully CAP compliant EAS equipment that is redundantly connected via satellite and internet to the state's existing EAS network. This integrated equipment will automatically export, via an USB or serial port, the full text of major EAS events to each station's existing EAS character generator. In

addition, this equipment can also be used as a standalone FCC certified CAP encoder/decoder device.

Michigan TV stations receive emergency alerts and information very fast. Alerts will be delivered to each equipped station at the same time as it is sent to the two local EAS Local Primary Stations for the area. Weather information from NOAA is equally as fast, available at virtually the same time as it is sent to NWS Weather Radio stations. The State of Michigan and many counties now have direct input to Michigan's EAS primary delivery system, which is encrypted, monitored and robustly designed.

### **Reduction of Master Control Operations through Automation**

As stations reduce master control operations through automation, or in hub-based operations, it is now often very difficult to have personnel available to manually compose character generated crawls on a 24 hour basis. This system, in conformance to FEMA IPAWS standards, will provide automatic delivery of an air-ready graphic crawl and word for word audio at any time of the day or night, without human intervention and sound local-- even if the master control of the hub is 1000 miles away.

### **Integrated CAP EAS Capabilities for Michigan Stations**

In 2012, virtually all Michigan TV stations received CAP EAS units that were fully integrated with the Michigan's satellite/internet CAP network. This package included:

- An IPAWS conformant
- FCC-certified integrated EAS encoder/decoder unit
- Satellite antenna
- LNB
- Monitor/keyboard/mouse
- All required software
- Standard installation
- Checkout
- Standard license and manufacturer's warranty

This bundle was seen as unique, as no other EAS encoder/decoder could internally host the satellite receiver and network software, while providing several other features required by television facilities.

### **Memo of Understanding (MOU)**

This equipment was supplied at no charge for the station's exclusive use. In exchange, the station signed an MOU with the following agreements:

1. The station is a full power TV station, licensed to a Michigan City.
2. The station agrees to follow all the provisions and event airing priorities of the State and Local EAS plans.
3. The station will provide both visual and audio emergency messaging consisting of the replacement of program audio with the full audio of the EAS message, while also providing (in open caption), the full text of the message, keyed over program video in an easily readable white font and crawled at the top of the screen (as is already presently

done for EAS messages).

4. This alert must be carried on the station's main and all multi-cast channels.
5. One unit will be supplied per call letter or for a common control point for more than one station.
6. The equipment is to remain in automatic operation 24/7/365. The only exception will be for those stations that are already in live severe weather coverage prior to the time the initial alert is received with all spoken information being closed-captioned for the hearing impaired.
7. To remain operational, this equipment must be connected to the internet at all times, as well as its satellite antenna. Proper operation of the network is monitored by the supplier, as well as at the Michigan EAS office, to insure both connections are functioning for each terminal on the system.

Therefore, it is understood, the station will maintain both working connections at all times: internet and satellite. To maintain satellite connectivity to the data supplier, full time system monitoring and continuing software updates, a small yearly license fee is to be paid by the station for years two through five. This is due at the anniversary date of the MOU and paid to the supplier of the service.

8. Failure to maintain the unit's operation, connectivity and warning procedures as listed above, will cancel the MOU. The equipment supplied under the agreement must then be returned with 15 days to the MAB for reassignment to another station.
9. The term of the MOU for this agreement is five years from the initial date of the MOU.

### **Michigan's Goals and Future Projects**

Michigan believes it is well ahead of the curve for EAS CAP implementation and its television stations will step up to take a leadership position and demonstrate their commitment to public warning of all our citizens, including those with special needs. Full Text messaging, now possible with CAP, allows the hearing impaired to read the entire emergency message; not just the cryptic event code, county and expiration time. At the same time, visually impaired persons will hear the entire message spoken to them.

The goal is to make Michigan, which has among the highest number of hearing impaired persons of any other state, the first state in the nation to implement this voluntary public warning enhancement under the leadership of Michigan's outstanding TV broadcasters.

To further indicate Michigan's commitment, an enhanced AMBER alert web based entry system is in development which will directly feed this state system, which in turn will provide fast alerting of abducted children to all broadcast and cable users, the State's AMBER web page, social media, electronic signage and CMAS.

Also, a pilot program is underway to demonstrate through a unique public/private partnership, the development of effective warning using IPAWS to the State's Arabic population, primarily in the Detroit area.

Over 25% of States across the country have recognized and purchased, as Michigan has, a dual path, integrated, monitored and encrypted system. This is an essential approach if we are to have a public warning system that is robust enough to continue to operate under infrastructure failures, which are to be expected in a major warning event and continue to grow and incorporate new technologies.

This section left intentionally blank

## 6 Recommendations/Best Practice Guidelines

### 6.1 Best Practice for Message Origination

As part of the Working Groups discussions, we observed the need for a set of best practices to guide both emergency managers and the systems development community in the process of CAP EAS message origination. While additional effort may be needed here to assist both emergency management and product developers, we assembled the following set of best practices as a starting point.

Before you begin, complete the following:

1. Complete the FEMA IPAWS Basic Course IS-247.a
2. Have a FEMA Certified CAP Origination Tool.
3. Have proper credentials and digital signatures for the CAP aggregator for which you are originating.
4. Review your State's FCC approved State Plan.



CAUTION: CAP is a very useful tool to originate and disseminate emergency information over a variety of platforms. CAP is very versatile, but in order for CAP messages to be processed by the Emergency Alert System on radio, television, cable, and other EAS Participants, there are fields in a CAP message that are mandatory for EAS processing, even if they are optional for CAP.

### 6.2 CAP Message Preparation

One of the purposes of this document is to assist in preparation of CAP messages that will be ultimately broadcast on radio, television, cable and other media. The CAP origination tool that you have should assist you in this process. Most references in this document are to the ECIG Recommendation for CAP EAS Implementation Guide which may be found on the ECIG website.

**Note:** Before any CAP message is processed by an aggregator, it must conform to OASIS CAP v1.2. The message should also conform to the current FEMA CAP Profile, which may be found at [www.fema.gov/](http://www.fema.gov/).

#### 6.2.1 EAS and CAP Audio

Audio is an important part of an EAS message, and CAP provides at least two methods for audio to be transported and inserted in a resultant EAS message.

An audio file can be inserted as a resource block, or the audio can be converted with Text to Speech from the description and instruction elements of the info block.

Although Text to Speech is an optional by current FCC Part 11 rules, the originator must realize that without one of these two methods, no audio will be present in the resultant EAS message. The only audible sound the listener will hear will be the EAS header codes, the Attention Signal,

and the End-of-Message signal. Note that IPAWS currently depends on Text-to-Speech conversion.

## 7 Mandatory CAP Message Checklist

	Mandatory CAP Address Block	Value	Notes
<input type="checkbox"/>	<alert>	---	Must be version 1.2 For example: <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
<input type="checkbox"/>	<alert><identifier>	---	Number or string uniquely identifying this message.
<input type="checkbox"/>	<alert><sender>	---	Globally unique - could be an email address.
<input type="checkbox"/>	<alert><sent>	---	Sent time in the format such as: "2012-07-25T16:49:00-07:00"
<input type="checkbox"/>	<alert><status>	Actual	The message will not be processed for EAS if the <status> is anything other than Actual.
<input type="checkbox"/>	<alert><code>	IPAWSv1.2	---
<input type="checkbox"/>	<alert><msgType>	Alert, Update or Cancel	---
<input type="checkbox"/>	<alert><scope>	Public	Although test Event codes, such as RMT, RWT, DMO, NPT, and NMN, may be used, the message will not be processed for EAS if the <scope> is anything other than Public.
<input type="checkbox"/>	<info><eventCode>	For example, CIV	One and only one eventCode, with a valueName of SAME and a 3-letter value is required.
<input type="checkbox"/>	<info><expires>	For example, 15	Must be greater than 0.
<input type="checkbox"/>	<parameter> <valueName>EAS-ORG </valueName> <value>CIV </value>	For example, CIV	Other values may be used, but "CIV" will be the most common.
<input type="checkbox"/>	<area><geocode> <valueName>SAME </valueName> <value>011011	For example, SAME=011011	The example is for the District of Columbia. At least one geocode is mandatory and more values may be provided, up to a maximum of 31 6-digit codes.  EAS messages will only process SAME values although other geographic information may be

	</value> </geocode>		included in a CAP message.
--	------------------------	--	----------------------------

## 8 Optional CAP Message Checklist

	<b>Address or Resource Book</b>	<b>Value</b>	<b>Notes</b>
<input type="checkbox"/>	<senderName>Human-readable name of agency or authority	---	Could be used for construction of alert text or other visual display.
<input type="checkbox"/>	<resourceDesc>	EAS Broadcast Content	Required if there is a Resource Block (for example, .mp3, .wav or streaming asset
<input type="checkbox"/>	<mimeType>	Audio/x-ipaws-audio, or video/x-ipaws-video, or video/x-ipaws-streaming-video	---

This space left intentionally blank

## 9 Best Practices

### 9.1 Best Practice for “Text to Speech”

A notification can be up to 1,800 characters and spaces in length, due to limitations on broadcast and cable video displays. Various CAP message origination tools may allow message originators to enter text that would be incorporated in the <headline>, <description> and/or <instruction> elements of a CAP message. This text would be rendered into synthetic speech by enabled CAP EAS devices, when such a message is received (assuming a voice audio file was not present).

#### 9.1.1 Message Originators

Message Originators should bear in mind that the content they input for text-to-speech would also be viewed on screen via TV and cable systems. For this reason, phonetic renderings of text should be avoided. To handle certain words, lexicons may need to be adjusted in CAP EAS receivers over time. In addition, message originators should avoid excessive use of acronyms or jargon.

#### 9.1.2 Alert Messages

Alert messages should optimally be succinct and to-the-point. If an alert message contains many words and characters, originators should make use of punctuation such as periods and commas. This can better pace the synthetic speech rendering of the sentences and helps the message content flow evenly and properly. It can also prevent run-on sentences and incorrect intonation, which may confuse the recipient and prevent him/her from understanding the content of the message.

#### 9.1.3 Entry of Address or Extensions

As a general convention, entry of addresses or extensions with a large number of digits may necessitate use of a space between each number.

For example, 32457 Safety Road should be entered in as 3 2 4 5 7 Safety Road.

#### 9.1.4 Reference Guidelines

Refer to the stylistic guidelines indicated in FEMA’s IS-247 training course (Lesson 2: Appropriate, Effective, and Accessible Alert and Warning Messages), as well as the style guide recommendations listed in the EAS Style Guide Appendix.

### 9.2 Best Practice for Audio

Audio is an important part of an EAS message, and CAP provides at least two methods for audio to be transported and inserted in a resultant EAS message. An audio file can be inserted as a resource block, or the audio can be converted with Text to Speech from the description and instruction elements of the info block. Although Text to Speech is an optional by current FCC Part 11 rules, the originator must realize that without one of these two methods, no audio will be present in the resultant EAS message; all a listener will hear are the EAS header codes, the Attention Signal, and the End-of-Message signal.

**Note:** IPAWS currently depends on Text-to-Speech conversion.



## 9.3 Best Practice for SSL Certificates

CAP/EAS devices are, for the most part, unattended, headless, embedded processor type systems. User maintenance interactions need to be limited. Some user installations are remote and do not have inbound internet access for security reasons.

### 9.3.1 Common Root Certificates

CAP/EAS devices will have a set of common Root CA certificates that are updated slowly. They may not be up to date with intermediate certificates. To avoid the necessity of loading intermediate certificates, in the larger world of desktops, it has become a common practice for a web server to send the server certificate as well as the various chained intermediate certificates. Similarly, in the specialized environment of CAP/EAS device, sending the chain will allow the CAP/EAS device to verify the chain of trust with only information from the SSL connection alone, as long the device has the applicable Root CA certificate.

If a CAP server wants to use HTTPS/SSL access and support the widest range of CAP/EAS devices, it must send all of the chained certificates (not including the Root CA) for SSL connections.

A CAP/EAS device must provide a means for its users to update the store of Root CA certificates, either by a firmware update, or a special certificate update.

CAP server owners should be aware that a change to the Root CA for its certificate chain, especially when a new CA is used, might cause CAP/EAS devices to not be able to connect to their server until the device manufacturers can issue an update.

In addition, self-signed certificates may not work with all CAP/EAS devices, and should be avoided.

This space left intentionally blank

## Appendix - EAS Style Guide

The EAS Style Guide is intended to assist CAP originators in formulating the optional fields of a CAP message that will be used for text-to-speech conversion, and display by character generators and various graphic platforms.

EAS Messages	All EAS messages are public; therefore, no information of a restricted or private nature should be included.
EAS Text	All EAS Text should support, not contradict information that may be contained in an encapsulated audio message that is a part of the CAP message.
FCC Mandatory EAS Text	Information derived from the FCC Mandatory EAS Text, i.e., originator, event type, time issued, expiration, duration, and sender ID will already have been displayed, so it is not necessary to repeat all of the information contained in the FCC Mandatory EAS Text EXCEPT for information of peculiar interest to the hearing impaired community.
EAS Phrasing	The EAS Text must be fairly formal in its phrasing, but should not make over-use of highly technical or discipline specific jargon. EASText should be for a target audience of third grade vocabulary and syntax.
Expression	Expression should be clear and concise.
Message Details	Details should be specific but must be limited to 1800 characters in order to fit within the constraints of a two-minute audio message. Important details should be repeated, but not lengthy.
Additional Message Details	EAS Text may be used to amplify or provide additional details about an emergency situation but should not be overly repetitive.
Description of Emergency	The first thing to convey is a brief description of the emergency; the second thing to describe is the action that the listener/viewer needs to take immediately; the third thing to describe is a pointer for additional details.
EAS Language	The EAS is designed to “wake up” listeners/viewer to an emergency condition, not provide a journalistic detail of events.

## Appendix References

- FCC EAS Rules (CFR 47 Part 11). Web:  
<http://ecfr.gpoaccess.gov/cgi/t/text{textidx?c=ecfr&rgn=div5&view=text&node=47:1.0.1.1.11&idno=47}>
- FCC Second Report and Order, in the Matter of the Review of the Emergency Alert System, EB Docket No. 04-296, Adopted: May 31, 2007
- FCC Fourth Report and Order, in the Matter of the Review of the Emergency Alert System, EB Docket No. 04-296, Adopted: September 15, 2011
- FCC Fifth Report and Order, in the Matter of the Review of the Emergency Alert System, EB Docket No. 04-296, Adopted: January 9, 2012
- CAP v1.2 USA IPAWS Profile v1.0 Committee Specification OASIS Emergency Management Technical Committee, October 2009.
- EAS CAP Industry Group (ECIG) Recommendations for a CAP EAS Implementation Guide, Version 1.0. Web: [http://eas-cap.org/ECIG-CAP-to-EAS\\_Implementation\\_Guide-V1-0.pdf](http://eas-cap.org/ECIG-CAP-to-EAS_Implementation_Guide-V1-0.pdf)