# Guide to Implementing the Integrated Public Alert and Warning System (IPAWS)



**October 2015**
**Version 1**

**TABLE OF CONTENTS**

| Version | Date | Changes |
| --- | --- | --- |
| Version 1 | October 2015 | First Version |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# EXECUTIVE SUMMARY

The Integrated Public Alert and Warning System (IPAWS) is "the nation's alert and warning infrastructure."

> *During an emergency, alert and warning officials need to provide the public with life-saving information quickly. The Integrated Public Alert and Warning System (IPAWS) is a modernization and integration of the nation's alert and warning infrastructure and will save time when time matters most, protecting life and property.*
>
> *Federal, State, local, tribal and territorial alerting authorities can use IPAWS and integrate local systems that use Common Alerting Protocol standards with the IPAWS infrastructure. IPAWS provides public safety officials with an effective way to alert and warn the public about serious emergencies using the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), the National Oceanic and Atmospheric Administration (NOAA) Weather Radio, and other public alerting systems from a single interface.[1]*

IPAWS in itself is not an alert and notification system; IPAWS is an input service to multiple alert and notification systems. Alerting is giving notice to the public that an event has occurred; this is often a short sound, action, or message. A notification has more information and usually has instructions for the public to try to protect them from the event. IPAWS uses open source protocols to receive an alert and/or notification message from an alerting authority and distributes the message to multiple dissemination systems.

To provide for the effective use of IPAWS, each entity should develop a plan for how it will use this tool to benefit the public that can incorporate existing and emerging alert and notification systems. To prepare an effective alert and notification plan, an agency (authority) must have a full understanding of the environment in which the authority operates. Every community is different in terms of needs and threats. The current situation will need to be explored, such as anticipated threats, populations, capabilities, and authority. Goals and objectives will need to be defined, and an official document prepared that includes details and roles and responsibilities. Memorandums of understanding (MOUs) with neighboring agencies may be necessary.

The selection of alert and notification systems should be based on information gathered during the planning process. Risks and community information will drive the alert and notification systems that are needed. In most cases, this will be a group of tools and systems that are used to notify various audiences and may be a physical system or a hosted solution. Functional requirements (statements of specific functions that a system or device must or should do) are then developed based on intended or expected functions needed by the authority. Requirements should be clear, verifiable, feasible, and necessary.

---

[1] Federal Emergency Management Agency. 2015. "Integrated Public Alert & Warning System." Accessed online September 28, 2015. http://www.fema.gov/integrated-public-alert-warning-system

Once the specifications of the needed functions are determined, one or multiple systems may need to be procured. These systems can be capital expenditures for fixed equipment or operational expenditures for maintenance or a service.

An alerting authority will also need authorization to access IPAWS, which is gained by following these steps:

- Select IPAWS-compatible software
- Apply for a memorandum of agreement (MOA) with the Federal Emergency Management Agency (FEMA)
- Apply for public alerting permissions
- Complete IPAWS web-based training

Once all forms have been completed, signed, and State-approved, IPAWS will issue a Collaborative Operating Group (COG) identification and digital certificate.

To use IPAWS and other alert and notification systems effectively, written documentation should be prepared that contains the information and actions needed to successfully alert and notify the public of emergencies and dangers.

All users must understand the systems and procedures, which is accomplished through initial and recurring training and exercises. IPAWS provides alerting authorities with access to a test COG for the use of training and exercises. This test COG can be programmed into many IPAWS authoring tools as a separate distribution environment.

Integrating alert and notification systems into regular operations also has benefits; it builds familiarity with systems, enables better thinking skills, and provides better response to emergencies. Use should include operation of the technology as well as forming messages and determining distribution channels, all of which will build skills.

While users require actual training on alert and notification systems, the public should also be "trained." Educating the public will increase the likelihood that the public will take actions to protect themselves when an actual event occurs.

IPAWS is a powerful tool for notifying the public with important lifesaving information. Creating an environment that supports alerting and notification communications is important. This document and associated templates can be used to develop an alert and notification plan and implement IPAWS into those plans. Templates can be modified in any way to address local situations to provide the best service to the public and responders.

# 1. OVERVIEW

The ability for local public safety professionals to be able to communicate with the public during emergencies is a critical function. The public looks to public safety officials to warn them of danger and inform them of actions to keep them safe.

The Integrated Public Alert and Warning System (IPAWS) is a very powerful tool.
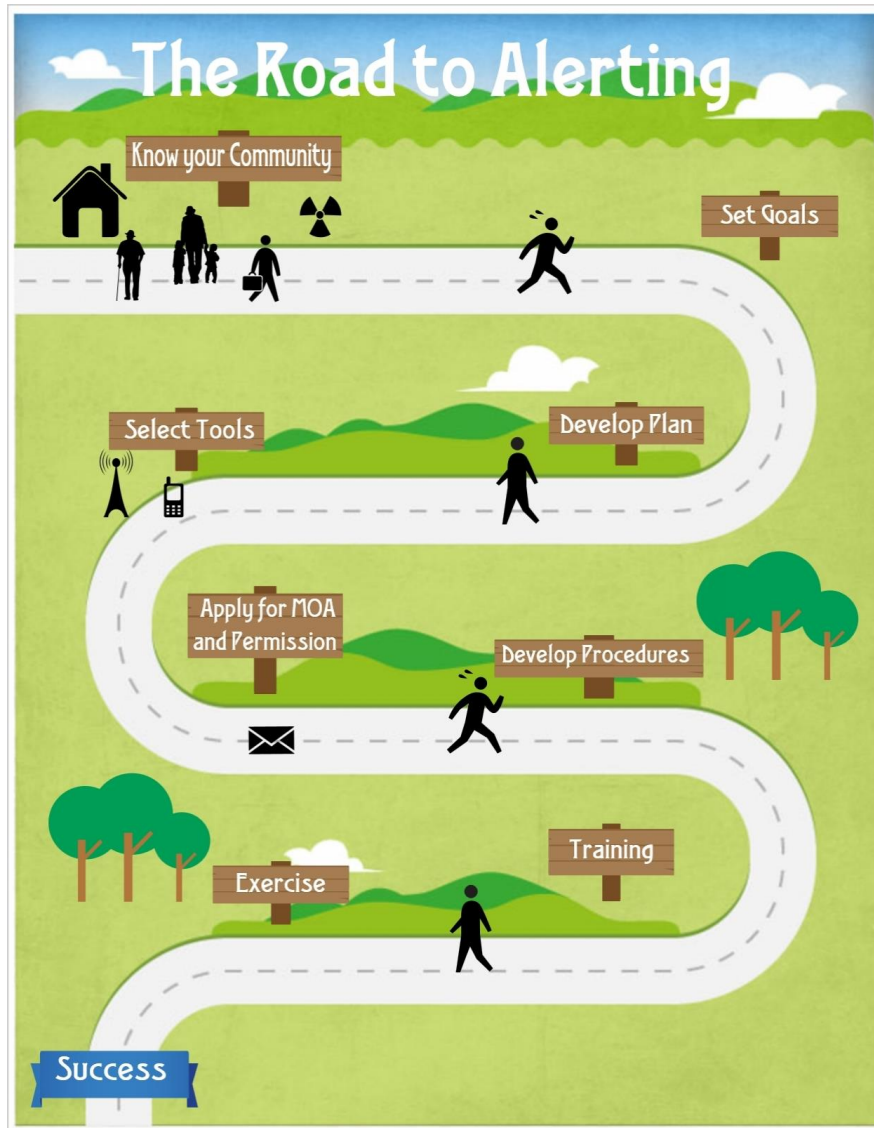
## 2. BACKGROUND

*"There is no substitute for accurate knowledge. Know yourself, know your business, know your men."*

Lee Iacocca

**References**

➢ Common Alerting Protocol. "v. 1.2, OASIS Standard CAP-V1. 2." (2010).
➢ Common Alerting Protocol, v. 1.2 USA Integrated Public Alert and Warning System Profile Version 1.0. (2009).
➢ National Weather Service, Operations and Services; Public Weather Services, NWSPD 10-5, Non-Weather Related Emergency Products Specification (Instruction 10-518, July 28, 2010)
➢ J-STD-101 – Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specifications
➢ http://www.fema.gov/integrated-public-alert-warning-system

IPAWS is a powerful tool for notifying the public with important lifesaving information. IPAWS was developed to primarily provide a national system for presidential messages, but the system is available for use by State, local, and tribal entities.

To provide for the effective use of this tool, each entity should develop a plan on how it will use IPAWS, which can incorporate existing and emerging alert and notification systems to benefit the public.

This document can be used to develop an alerting and notification plan and to implement IPAWS into those plans. This plan is used to document the current situation, goals, and procedures to implement and manage alerting and notification systems. This template can be modified in any way to address local situations to provide the best service to the public and responders.

FEMA manages and funds the core IPAWS infrastructure but not the alert origination tools or distribution channels. IPAWS is designed to provide a single authenticated entry point to the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), the National Oceanic and Atmospheric Administration (NOAA) Weather Radio All Hazard, and other alerting systems. Some communities use older emergency notification systems, which may require an interface to IPAWS for interoperability.

Creating an environment that supports alerting and notification communications is important. Some of the things that can provide this environment are as follows:
- Plans: Pre-established plans outline what systems will be used by whom. These should include primary and alternate systems as well as systems used by other agencies.

- Policies and Procedures: Clear policy and procedure delineate who, when, how, and why various communications will take place.
- Training: Recurring training on the use of the systems will improve the skills of the users. It is important to have multiple people trained on all systems.
- Exercise: Use of these systems on a regular basis will increase effectiveness.

This is a constant process with plans trained, exercised, and refined regularly. This process also helps to keep the information fresh in the minds of the users.



## 2.1. PLANNING PROCESS

The planning process is used on a regular basis by emergency management. The same process used to develop the Emergency Operations Plan can be used. A good guide to the development of plans is FEMA's *Developing and Maintaining Emergency Operations Plans, Comprehensive Preparedness Guide (CPG) 101*, Version 2.0, November 2010. The following graphic from that guide outlines this process.

| STEP 1 Form a Collaborative Planning Team | STEP 2 Understand the Situation | STEP 3 Determine Goals and Objectives | STEP 4 Plan Development | STEP 5 Plan Preparation, Review, & Approval | STEP 6 Plan Implementation & Maintenance |
|---|---|---|---|---|---|
| Identify Core Planning Team | Identify Threats and Hazards | Determine Operational Priorities | Develop and Analyze Course of Action | Write the Plan | Exercise the Plan |
| Engage the Whole Community in Planning | Assess Risk | Set Goals and Objectives | Identify Resources | Review the Plan | Review, Revise, and Maintain the Plan |
|  |  |  | Identify Information and Intelligence Needs | Approve and Disseminate the Plan |  |

## 2.2. COMMUNICATIONS CYCLE

Communications is more than a piece of equipment or technology. Understanding the communications cycle is the first step in reliable and effective communication. As the sender of information to various groups, you need to understand how the audience and the medium you use to send messages have an impact on the effectiveness of any communication.

**Communications Cycle**

Message
Medium
Sender
Receiver
Feedback
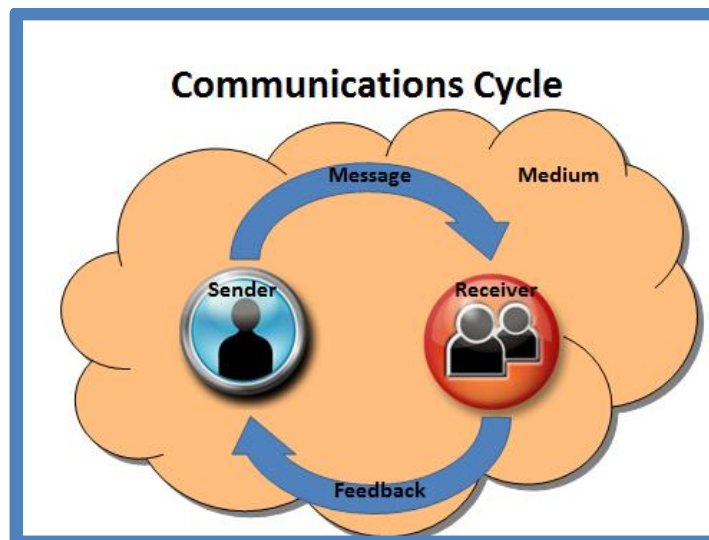
The message is only part of the communication. Many people place additional meaning on the medium used to transmit the message. An extreme example is the message "the Martians are coming" on a sign held by a person on the street in a major city. The audience will place a certain meaning on that

message, but if it is stated in a press conference on television from a government office, the same message is given very different meaning.

To help communications be effective and reliable, users must be familiar with the various systems available and the impact of each system and audience. If a message is not understood by the audience or the audience attaches meanings that are not intended, effective communication has not occurred. The communications needed during an emergency require the audience to receive, understand, and take any necessary protective action in response to the message.

## 2.3. UNDERSTANDING ALERT AND NOTIFICATION

Alert and notification are two different actions, but both are important to protect the public. Alerting is giving notice to the public that an event has occurred; this is often a short sound, action, or message. For a radio listener, the alert would be the EAS tones and headline that precedes an EAS message.

A notification has more information and usually has instructions for the public to try to protect them from the event. For a radio listener, this would be the description and instructions in the EAS message.

| Alert | Notification |
|---|---|
| A warning signal to be ready | Information on event and actions to take |

Understanding the difference between alert and warning as well as the capabilities of the alert and notification systems is needed to provide an effective, reliable, and rapid means of communications to the public in the event of natural or human-caused disasters. Alerting authorities must understand both alerting the public of a danger and notification of what actions to take.

## 2.4. UNDERSTANDING HOW IPAWS WORKS

The alert and notification systems in the United States have been developed over time. In the early days of the Cold War, it was realized that there needed to be a rapid way to alert the public of impending attack.

This need was addressed in a basic way with the CONtrol of ELectromagnetic RADiation (CONELRAD) system. CONELRAD was a basic system where participating stations would get a nationwide notice and then locally initiate a sequence of pre-defined actions to warn the public.

The Evolution of Emergency Broadcasting

| 1951 - 1963 CONELRAD | 1963 - 1997 EBS | 1997 - 2006 EAS | 2006 IPAWS |

Originally called the "Key Station System," the **CON**trol of **EL**ectromagnetic **RAD**iation (CONELRAD) was established in August 1951.

Participating stations tuned to 640 & 1240 kHz AM and initiated a special sequence and procedure designed to warn citizens.

EBS was initiated to address the nation through audible alerts. It did not allow for targeted messaging.

System upgraded in 1976 to provide for better and more accurate handling of alert receptions.

Originally designed to provide the President with an expeditious method of communicating with the American Public, it was expanded for use during peacetime at state and local levels.

EAS jointly coordinated by the FCC, FEMA and NWS.

Designed for President to speak to American people within 10 minutes.

EAS messages composed of 4 parts:
- Digitally encoded header
- Attention Signal
- Audio Announcement
- Digitally encoded end-of-message marker

IPAWS modernizes and integrates the nation's alert and warning infrastructure.

Integrates new and existing public alert and warning systems and technologies

Provides authorities a broader range of message options and multiple communications pathways

Increases capability to alert and warn communities of all hazards impacting public safety.

Over time these systems evolved to allow for more message flexibility and the ability to target specific geographic areas.

IPAWS in itself is not an alert and notification system. IPAWS is an input service to multiple alert and notification systems. **This is the power of IPAWS.**

IPAWS uses open source protocols to receive an alert and/or notification message from an alerting authority and distribute the message to multiple dissemination systems.


IPAWS Architecture
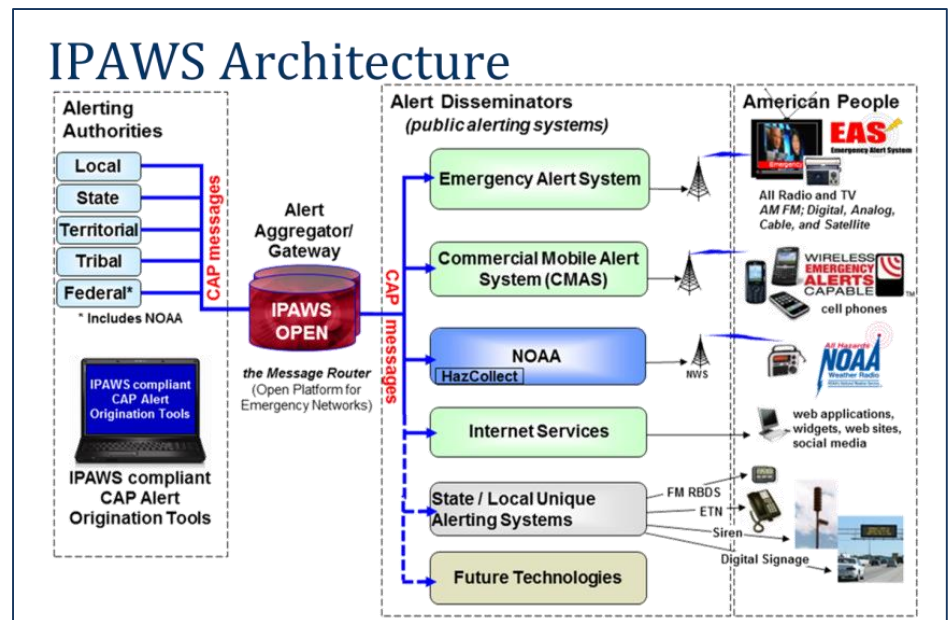
| System | Distribution | Notes |
|---|---|---|
| EAS | Pull | Not required to broadcast local messages |
| WEA | Push | Limited message length |
| National Weather Service Radio | Push | Additional permissions required |

| System | Distribution | Notes |
|---|---|---|
| All Hazards Information Feed | Pull | Varies by systems |

### 2.4.1.  Common Alert Protocol

*The Common Alerting Protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience.[2]*

The CAP standard is an internationally recognized standard for information exchange published by the Organization for the Advancement of Structured Information Standards (OASIS). OASIS is a nonprofit consortium that drives development and adoption of open global information standards.

CAP is a set of common published Extensible Markup Language (XML) tags that allow the formatting of messages in a common and open format that can then be used by various systems. CAP allows the user to format messages and add links to other information such as audio, video, and pictures.

A CAP message has many available data elements; not all elements are used by IPAWS, and some are required but not used in the published message. Each dissemination channel will have different data elements that are required and used. For example, a WEA message requires a valid severity element but does not use this in the message. WEA does not formally require the use of CMAMtext as part of a CAP <parameter>; however, if it is not used, the 90 characters that are broadcast are derived from other CAP message elements. (Section 5.3, Develop Message Templates, in this document has additional information.)

A sample CAP message can be found on the following page.

---

[2] "Common Alerting Protocol Version 1.2: OASIS Standard." 2010. Accessed online September 28, 2015. http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html

```
<alert>
    <identifier>MSU-3292aca8-949f-4336-a825-ecf6872a8405</identifier>
    <sender>ClarkCountyEOC</sender>
    <sent>2010-07-20T04:41:00-07:00</sent>
    <status>Actual</status>
    <msgType>Alert</msgType>
    <scope>Public</scope>
    <info>
        <category>CBRNE</category>
        <event>Civil Emergency Message</event>
        <responseType>Evacuate</responseType>
        <urgency>Immediate</urgency>
        <severity>Severe</severity>
        <certainty>Possible</certainty>
        <headline>The danger of further dispersal of the radiation from the initial attacks, or new
            attacks, has passed and further attacks are not anticipated</headline>
        <description>This is a demonstration only message. The danger of further dispersal of the
            radiation from the initial attacks, or new attacks, has passed and further attacks are not
            anticipated at this time</description>
        <instruction>Do not take action based on this message.</instruction>
        <area>
            <areaDesc>National Emergency</areaDesc>
            <polygon>47.57652571374621,-66.884765625 25.562265014427492,-79.892578125
                32.32427558887655,-119.619140625 49.32512199104001,-125.947265625
                49.49667452747044,-97.03125 49.210420445650286,-89.384765625</polygon>
        <geocode>
            <valueName>SAME</valueName>
            <value>011001</value>
        </geocode>
        </area>
    </info>
</alert>
```

### 2.4.2.  IPAWS-OPEN

The IPAWS aggregator or Open Platform for Emergency Networks (IPAWS-OPEN) is operated by
FEMA, which provides credentials to authorized alerting authorities. Local jurisdictions also require
State approval as an alerting authority. IPAWS-OPEN receives messages from alerting authorities and
performs several validation checks on the message.

- Is the message from a valid system? IPAWS-OPEN verifies a valid certificate from the sending
  device.
- Is the message formatted properly? IPAWS-OPEN validates the message follows the CAP v1.2
  format.
- Does the authority have permission to send this type of message? IPAWS-OPEN validates the
  message content and type against IPAWS permissions from the authority's application.
- Does the authority have permission to send to the selected dissemination channels? IPAWS-
  OPEN validates the message destination against IPAWS permissions from the authority's
  application.
- Lastly, IPAWS-OPEN verifies the message format for each dissemination channel. Each
  dissemination channel has different data elements and formatting rules for messages.

After all validations have been successfully authenticated, the message is sent to the dissemination channels.

### 2.4.3. EAS Feed

The alert authority must be approved to send to the EAS feed, and the message must have an incident type that is approved and listed on the COG agreement. Each message then must also be in an EAS-valid CAP format.

IPAWS will post valid messages to the EAS feed, a secure server where messages can be retrieved by EAS-participating broadcasters. Each broadcaster is required to have IPAWS-capable equipment to periodically poll the EAS feed for a message and retrieve messages as needed.

Each broadcaster configures the IPAWS-capable equipment at its station to retrieve messages at certain intervals. This interval is recommended to be no more than 2 minutes but, by Federal Communications Commission (FCC) rule, can be as long as 8 minutes.

Broadcasters are only required to broadcast Presidential alerts; local and weather messages are voluntary. The equipment can be programmed to immediately broadcast, ignore, delay, or require a person at the broadcast station to review and take action to broadcast a local or weather message.

The EAS CAP message allows the alert authority to include a link to other data, such as pictures and audio recordings. This requires the alerting authority to have a server accessible from the Internet for the broadcaster to retrieve this information. Many IPAWS software vendors include this in their software or service.

Section 3.1.4, Commercial Broadcaster Capabilities, in this document has additional information on the operation of EAS.

### 2.4.4. WEA

IPAWS is the only way to send Wireless Emergency Alerts (WEA). The alert authority must be approved to send to the WEA, and the message must have a type that is approved and listed on the COG agreement. Each message then must also be in a WEA-valid CAP format.

IPAWS sends the valid message to participating wireless providers. WEA is a voluntary program; while the four major carriers and many small carriers participate, not all wireless providers do. Alerts are received by participating wireless providers, who process the messages and broadcast to WEA-capable wireless phones.

Participating wireless providers are required to send messages to a county area or larger based on county-level geocodes (usually Federal Information Processing Standard [FIPS] codes), but virtually all carriers will narrow the broadcast to cell towers broadcasting within a geographic circle or polygon if the

circle or polygon is included in the CAP message. The specific method by which cell towers are chosen for broadcast may differ between carriers.

The WEA message is sent to targeted tower control channels and is not affected by other calls or texts on the system. WEA-capable phones that are connected to a targeted tower's signal will receive a WEA alert. WEA alerts can be re-transmitted at intervals set by the wireless providers, so if a WEA-capable phone enters the geo-targeted area after an alert is first sent, that WEA-capable phone will still be able to receive the WEA for as long as the WEA is active.

Receipt of the message by a specific phone is dependent on the phone being a WEA-capable phone. Each wireless provider lists its capable phones on its website. The phone will also allow a user to turn off imminent threat and AMBER Alert messages but not Presidential alerts. Lastly, a WEA message will not interrupt a call in progress or active data session. On some phones, if there is a data session running—even in the background (such as a weather application)—the WEA will not interrupt until the data session has ended.

Section 3.1.5, Wireless Provider Capabilities, in this document has additional information on the operation of WEA.

### *2.4.5. NWEM*

The alert authority must be approved to send to Non-Weather Emergency Messages (NWEMs) to the National Weather Service (NWS) All-Hazards Emergency Message Collection System (HazCollect), and the message must have a type that is approved and listed on the COG agreement. Each message then must also be in an NWEM-valid CAP format. Alert authorities require additional permissions from NOAA to post NWEM alerts to the NWS radio system. (Section 5, Apply for COG Status, in this document has application instructions.)

IPAWS sends the CAP message to the NOAA system. Messages are then validated by NOAA, which requires additional location elements that match the NOAA areas. This is used to determine the broadcast of the message. Most IPAWS systems that are NWEM-capable will permit pre-validation of these elements. NOAA will then broadcast the message over the NWS radio system.

Some technical issues are being resolved. Due to the duplication of the legacy EAS and the legacy NWS Weather Radio with the IPAWS feed, there is a chance for duplicate messages. The NWEM feed may not be available to local alerting authorities. NOAA has tested some vendor solutions for compatibility, but this list changes often. It will be necessary to ensure your systems are capable and approved by NOAA. Contact the local forecast office or IPAWS Program Management Office (PMO) for status updates or to learn more.

### 2.4.6. IPAWS All-Hazards Information Feed

IPAWS will send messages that are marked "public" to an additional information feed. This feed operates similar to the EAS feed by making messages available to an approved user for retrieval.

Various groups, organizations, and vendors apply for a MOA with IPAWS to gain access to this feed. They then publish the information to their third-party systems. These systems may be free, such as a mapping website, or subscriber-charged, such as a situational awareness application.

## 3.  ALERT AND NOTIFICATION PLANNING

> *"Failing to plan is planning to fail"*
>
> *Benjamin Franklin*

<div style="background-color:green">

**References**

- ➢ Developing and Maintaining Emergency Operations Plans, Comprehensive Preparedness Guide (CPG) 101, Version 2.0, November 2010
- ➢ Local Emergency Operations Plan
- ➢ State EAS Plan
- ➢ FEMA IS-2001 Threat and Hazard Identification and Risk Assessment (THIRA) Course
- ➢ Census data at: https://www.census.gov/
- ➢ Code of Federal Regulations (CFR) 47 Part 11 — Emergency Alert System
- ➢ CFR 47 Part 10 — Commercial Mobile Alert System

</div>

### 3.1.   UNDERSTANDING THE SITUATION

To prepare an effective alert and notification plan, the authority must have a full understanding of the environment in which the authority operates. Every community is different in terms of needs and threats. The best place to start this process is the community's Emergency Operations Plan (EOP). This plan will include much of the information needed to make decisions in the alert and notification planning process.

### *3.1.1.   Community Threats*

The community's EOP will have information on anticipated threats. For alert and notification planning, these threats should be categorized with information on the following:

- **Threat:** The risk must be described.
- **Preparation time:** Does the risk provide advance warning that the event is approaching, such as for a hurricane? Time considerations depend on the nature of the event and should be listed in hours.
- **Onset:** When the event occurs, how much time is available for an alert and notification warning?
- **Geographic Impact Area:** If the event occurs, what is the extent of the area that would be affected?
- **Severity:** If the event happens, how severe is the impact to life and property?
- **Likelihood:** What is the percentage of probability of this risk occurring?

| Example Risk Analysis | |
|---|---|
| *Threat:* | *Tornado in a tornado prone area* |
| *Preparation Time:* | *0 to 24 hours* |
| *Onset:* | *1 to 15 minutes* |
| *Geographic Impact Area:* | *Path from ¼ to 1 mile wide by ½ to 5 miles long* |
| *Severity:* | *Severe* |
| *Likelihood:* | *99%* |

### 3.1.2. Community Populations

Understanding the intended audience will help effective communications and aid in selecting the best application or system for the communication. It is important to understand that to provide effective communications in an emergency, the user may need to use more than one system.

- **Residents:** Residents, as an audience, are usually not trained, but they often have some knowledge from public education efforts. This audience may be able to understand short messages, such as "SIP," which means Shelter in Place, based on their knowledge.
- **Visitors:** Visitors, as an audience, usually have no training or knowledge of the area or dangers. This audience will usually need more specific information than a resident.
- **Access and Functional Needs:** Access and functional needs audiences will have similar characteristics as residents or visitors but will require additional considerations during communications. Access and functional needs groups include speech and hearing impaired, non-English speaking, elderly, or youth. Each group may have different needs; understanding the populations within or transiting an area is important when developing messages.
- **Critical Facility Staff –** Critical facility staff, as an audience, usually have the added responsibility of being responsible for infrastructure (e.g., schools, nursing homes, and water treatment plants) or people in their care. This audience will generally need more information than the general public and will often need more time to take necessary actions to save lives and protect property. It takes longer to move 200 people to shelter than a 5-person family.
- **Media:** The media is a conduit to the public and may have additional information needs above what they report to the public. Many reporters try to fully understand the situation to present the information in context and put the information into their own style.

A list of community populations should be developed that includes the following information:

- **Population:** This is the group of people that may be affected by an incident. This group should be segmented by more than just "visitor" or "resident." For example, "visitor" can be someone travelling on a highway or vacationing at a park.

- **Available Communications Media:** This is a list of available media that may reach this group. Communications media can include voice, text, and specific message dissemination systems like EAS or WEA.
- **Language:** This is the language in which the group is fluent and can include foreign languages as well as American Sign Language (ASL).
- **Notes:** This encompasses other information that may be of importance to the planning process. This can include seasonal information for groups that are in the area only certain times, such as migrant workers, fairs, etc.

### 3.1.3. Community Capabilities—Alert Technologies

Each available system has advantages and disadvantages. Selecting the proper technology mix to get the best coverage of messages is important. Several currently available systems and their key features are listed on the following page. These applications can be used as part of an alert and notification plan to send messages based on the availability of the system, the user's ability, and the intended audience.

These communications systems can be one-way or two-way. One-way messages must be very clear and include information that the sender may not use with other communications systems. One-way messages should always clearly state who, what, where, when, and why; use clear and simple language; and include where to get more information.

| Application | Alert (A), Notification (N), or Both (A/N) | Intended User/Audience | Time Frame | Description |
|---|---|---|---|---|
| Sirens | A | Outdoor and open space public | Immediate | • One-way system for alerting the public of emergencies<br>• Limited information available<br>• Must be followed up with where to get detailed information<br>• Visitors may not know what messages may mean |
| Public Address (PA) | A/N | Indoor and outdoor open space public | Immediate | • One-way system for alerting the public of emergencies<br>• Limited information available<br>• Must be followed up with where to get detailed information<br>• Visitors may not know what messages may mean |
| Tone Alert Radios (TARs) | A/N | Indoor Public | Immediate | • One-way system that can be used to alert the public<br>• Provides some additional information of actions required<br>• Limited to fixed sites that have these devices |
| Emergency Telephone Notification Systems (ETNS) | N | Landline or pre-registered wireless phones | Near-term | • One-way system that can be used to notify users of actions needed<br>• Systems are often best effort and have some latency based on the system and usage at the time of use<br>• Transmission of Teletypewriter (TTY) signals required for equal access |
| Legacy EAS | A/N | Commercial Media watching public | Near-term | • One-way system for alerting the public<br>• Provides a limited amount of information<br>• Constrained by available types of messages the system allows<br>• Local messages are not required to be broadcast by the media outlets |
| IPAWS | | Various – See Below | Immediate | • Acts as a gateway to several other alerting methods<br>• Allows users to create a single message that is disseminated via multiple methods |

| Application | Alert (A), Notification (N), or Both (A/N) | Intended User/Audience | Time Frame | Description |
|---|---|---|---|---|
| IPAWS – EAS | A/N | Commercial Media watching public | Near-term | <ul><li>One-way system for inputting messages to other systems</li><li>Used for alerting the public and providing a limited amount of information</li><li>Constrained by available types of messages the system allows.</li></ul> |
| IPAWS – WEA | A | Wireless phone public | Immediate | <ul><li>One-way system for alerting the public</li><li>Provides a limited amount of information</li><li>Constrained by the available types of messages the system allows</li><li>Uses cellular radio broadcast of a short text to wireless phones and, as such, may reach visitors more easily</li><li>Not all phones receive these messages</li><li>The public can disable this from their phones</li></ul> |
| IPAWS – NWEM | A/N | Weather Radio users | Immediate | <ul><li>One-way system for alerting the public</li><li>Allows more detailed information</li><li>Constrained by available transmitters in the area</li><li>Public has to tune to these stations</li><li>Added benefit of using weather radio county codes for notifications</li></ul> |
| IPAWS – All-Hazards Information Feed | N | Private service users | Near-term | <ul><li>Used by several commercial systems</li><li>Include popular mapping and search engines and commercial alerting services</li></ul> |
| Highway Traffic Radios | A | Traveling Public | Near-term | <ul><li>One-way system for alerting the public</li><li>Allows more detailed information</li><li>Constrained by available transmitters in the area</li><li>Public has to tune to these stations</li></ul> |

| Application | Alert (A), Notification (N), or Both (A/N) | Intended User/Audience | Time Frame | Description |
|---|---|---|---|---|
| Alert Translation Services | A/N | Non-English Speaking/Deaf and Hard of Hearing Public | Near-term | • One-way system usually accepts the IPAWS feed<br>• Translates to ASL or other languages and then posted to a public website or sent via ETNS |
| Roadside Message Boards | A | Traveling Public | Near-term | • One-way system for alerting the public<br>• Provides a limited amount of information<br>• Constrained by size of the sign and ability of a driver to read the sign |
| Route Alerting | A/N | Public in fixed locations along the route | Near-term | • Generally a one-way system for alerting the public along a route<br>• Takes time and resources to cover relatively small areas<br>• Sound (e.g., sirens) may not penetrate modern buildings |
| Cable system interrupt | A/N | Cable viewers | Immediate | • One-way system for alerting the public<br>• Allows more detailed information<br>• Constrained by the available access<br>• Being replaced by other more-focused systems as cable system areas expand |
| Social Media | N | Internet Connected Public | Delayed | • Used to provide information to the public and sample public reactions<br>• Can help reduce rumors<br>• Can be used in some cases as a method to get reports from the public |
| Press Release | N | Media | Delayed | • One-way system that allows for more information to be sent to the media<br>• Information is sent, but that does not mean it will be relayed to the public |
| Press Conference | N | Media | Delayed | • Two-way system that allows the media to give feedback and expand their understanding of the situation<br>• Not all information may get to the public |

### 3.1.4. Commercial Broadcaster Capabilities

Commercial broadcasters are not required to broadcast local alerts. It is important for the alerting authority to understand the plans and systems of the local broadcasters with which they work. Often, these broadcast areas cover multiple jurisdictions and cannot deliver messages to sub-county or small areas. All messages are broadcast to the entire broadcast area. Broadcasters include television, radio, cable television systems, and satellite.

In the legacy EAS system, messages were pushed to broadcasters over the radio in most cases. The messages are pushed from an origination source such as the Federal Primary Entry Point (PEP) stations or a local State Primary (SP) or Local Primary (LP) station. Each message was pushed to an expanding chain of stations, and each broadcaster was required to monitor another station up the chain in accordance with the State EAS Plan.

With IPAWS, broadcasters pull messages from the IPAWS-OPEN feed. The broadcaster's equipment polls IPAWS-OPEN for new message headers on a periodic basis set by each broadcaster. If the equipment identifies a message header that is targeted within the broadcaster's area(s), the equipment will then request the full message.

The alerting authority should identify the broadcasters that service the jurisdiction and other information such as the following:
- Contact information (24x7)
- Technical contact for system configuration and troubleshooting
- Configuration of EAS equipment, including the following:
  - Source feeds monitored
  - Rebroadcast methods per event type allowed to alerting authority (automatic, manual, none)
  - Time duration between polls of the IPAWS feed to pull alerts
- How messages are processed by station equipment

Appendix C contains a model EAS survey form that can help collect some of this information.

### 3.1.5. Wireless Provider Capabilities

Participating wireless providers are required to broadcast valid messages that are sent by public safety officials and delivered by IPAWS-OPEN. The message is pushed to participating wireless providers by IPAWS-OPEN. The wireless provider then processes the message to determine the targeted towers to send the message for distribution. The wireless provider's system sends the message to targeted towers and then sends the message to the handsets on their network that are connected to the targeted towers.

Providers are required to deliver messages to an area at least as small as a county. However, many providers have voluntarily agreed to deliver messages to sub-county areas based on the CAP area element. The CAP area element includes a geographic polygon created by the sender. When an

alerting authority adds an area element to the CAP message, the wireless providers use that element to determine the target towers to which to send the message.

The provider examines the message and applies the provider's processes to the message to determine where to send the message. The process followed by providers to determine which towers varies by provider but falls into three methods currently.
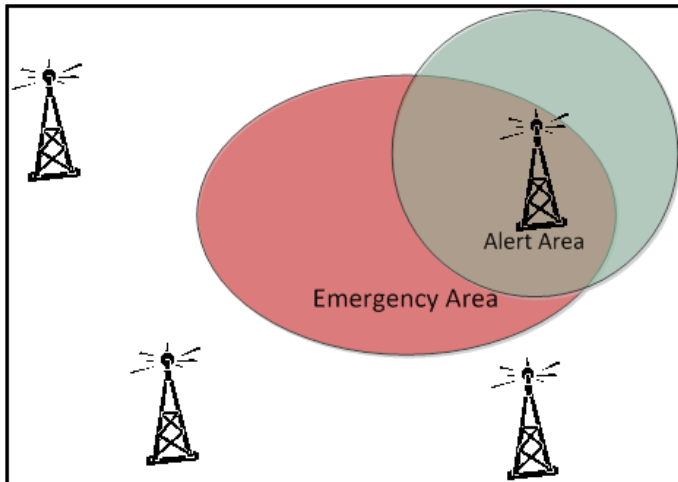


**Method 1**
All towers that are physically located within the alert area are selected to broadcast the message. Depending on the location of the towers, this can lead to not alerting a large area and alerting some areas that are not at risk.
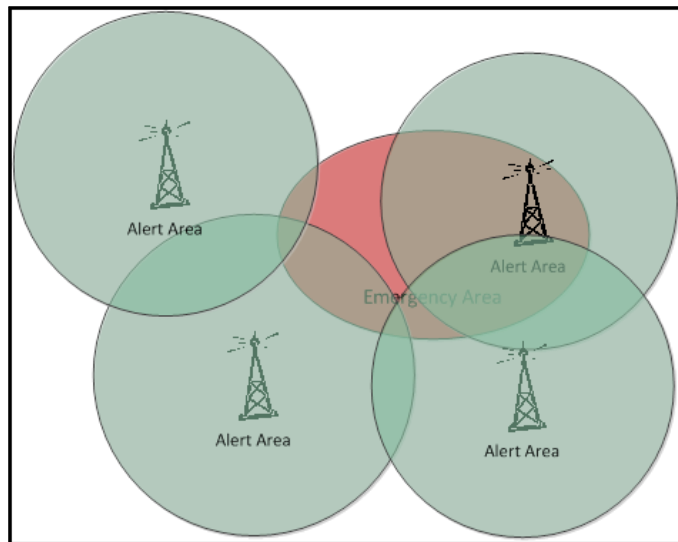


**Method 2**
All towers that have a coverage area that is within the alert area are selected to broadcast the message. Depending on the location of the towers, this can lead to alerting large areas that are not at risk and not alerting some at-risk areas.

**Method 3**
All sectors that have a coverage area within the alert area are selected to broadcast the message. Depending on the location of the towers, this can lead to alerting areas that are not at risk and not alerting some areas that are at risk.
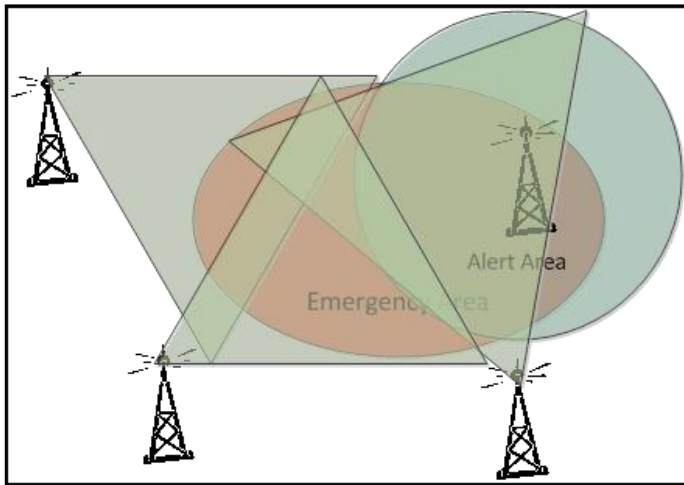
The wireless provider broadcasts the message to phones connected to the towers selected. This transmission uses control systems and is not affected by traffic on the system. If a person's phone is currently in use—including voice calls or data sessions—during the broadcast, the message will not be received, even if that session is in the background, such as a mapping application.

The wireless provider can set the system to automatically re-transmit the message at set times if the duration of the message is still valid. The interval of any re-transmission may vary from provider to provider.

It is important to understand that the WEA system uses cellular broadcast technology and radio transmissions and will not provide a specific addressable location capability. Wireless providers' radio systems are continually being adjusted to provide coverage; consequently, radio power, coverage, and availability change frequently. There will always be some dead spots and some over-alerting by the nature of the system.

Understanding the location of towers and how they will send messages aids the alerting authority in developing the alerting plan and procedures to use IPAWS. Appendix D contains a model WEA survey. Most of this information should already be available to the 9-1-1 authority.

### 3.1.6. Authority

Research on State and local authorities for alerting and delivering messages to the public should be conducted. Authority may not be listed as a clear role in State or local statues or rules but can often be derived from the highest elected official in most cases as a default.

Once the alerting authority is established, determine if that authority has been delegated. Some States will delegate the authority to alert the public from the governor to an agency or the secretary of a cabinet-level agency.

Once existing lines of authority are documented, State and local governments should determine the best method to alert the public. Some questions to ask when determining this are as follows:

- Who can make the determination of when to alert the public?
- Who can determine what message to use to alert the public?
- Who has access to the equipment needed to alert the public?
- Who will be available on a 24-hour basis to alert the public?

Once a determination of the best way to alert the public has been made, the person or agency with authority should delegate that authority in writing. This can be done with specific guidelines or policies that can include the following:

- Ability or non-ability to further delegate
- When the authority can be used
- What actions can be performed with the authority
- What notifications must be made if authority is used

When delegating authority, it is often best to delegate to a position or agency within the organization, such as the director of communications, rather than a specifically named person. This will provide better succession abilities in the future.

### 3.1.7.  IPAWS Authority

Development of IPAWS added another level of authority to the environment. IPAWS was developed to allow for national command alerting but has been made available to State, local, and tribal governments.

To gain access, the State or local entity must enter into an agreement with FEMA; requests by local governments must be approved by the State. This process grants the State an additional responsibility and authority over the use of a specific alerting technology.

### 3.2.  GOALS AND OBJECTIVES

As a community begins the planning process, identifying why the plan is needed is important. Developing a plan just to have a plan and then put on the shelf a waste of time and resources. A good plan must have a clear purpose defined by the goals and objectives that drive the planning process. The *Developing and Maintaining Emergency Operations Plans, Comprehensive Preparedness Guide* defines goals and objectives as:

*Goals are broad, general statements that indicate the intended solution to problems identified by planners during the previous step. They are what personnel and equipment resources are supposed to achieve. They help identify when major elements of the response are complete and when the operation is successful.*

*Objectives are more specific and identifiable actions carried out during the operation. They lead to achieving response goals and determining the actions that participants in the operation must accomplish. Translating these objectives into activities, implementing procedures, or operating procedures by responsible organizations is part of planning. As goals and objectives are set, planners may identify more requirements that will feed into the development of courses of action as well as the capability estimate.*[3]

**Example Goals and Objectives**

*__Goal 1:__ Alert the residents of the county of impending or ongoing emergency.*

*__Objective 1.1:__ Activate appropriate Tone Alert Radios within 2 minutes of determination of risk*
*__Objective 1.2:__ Notify School district by radio within 2 minutes of determination of risk*

Setting goals and objectives is based on the environment, the community, and the resources available. Some communities, such as Chemical Stockpile Emergency Preparedness Program (CSEPP) communities, may have goals established based on the risks. Other communities, such as Radiological Emergency Preparedness Program (REPP) communities, may have goals established by Federal rules.

Questions to ask when developing this section include the following:
- What are the threats to the community?
- What are the populations of the community?
- What is the availability of alerting systems in the community?
- Are there any prescribed goals for the identified threats?
- What objective will accomplish the goals?

## 3.3. PLAN DEVELOPMENT

After gathering an understanding of the current situation and setting goals and objectives, a plan will be developed to accomplish goals and objectives in the current environment. It is important to base the plan on the current situation. Plans that include systems or situations that do not exist today will adversely affect the ability to use the plan. A draft plan can be developed to plan for incorporating new technologies such as IPAWS.

---

[3] Federal Emergency Management Agency. 2010. *Developing and maintaining emergency operations plans: Comprehensive Preparedness Guide (CPG) 101*, version 2.0

Plans are living documents and should be reviewed, updated, and improved over time. The plan should have a scheduled review timeframe, and new systems should be added to the plan as needed but not until the new systems are available.

### 3.3.1. Components of an IPAWS Plan

The components of an alert and warning plan should include the following:
- Introductory material
- Situation, authority, and purpose
- Alerting plan detail
- Roles and responsibilities
- Appendices

A model public alert and notification plan can be found in Appendix E. Additional examples and information can be found at www.fema.gov/informational-materials.

#### Introductory Material

The introductory material establishes the plan as an official document, and provides a summary of the document. This section consists of the following:
- **Promulgation Document/Signature Page:** The promulgation document is usually a cover letter from the alerting authority that adopts the plan and gives the plan a legal basis.
- **Record of Change:** The record of change is used to track the date, reason, and a summary of what has changed over time.
- **Table of Contents:** The table of contents is a reference to guide the reader to sections of the plan.
- **Executive Summary:** The executive summary is a high-level summary of the plan that covers the basic plan and authority. The executive summary will also be the cover page that includes the information that the alerting authority has adopted the plan.

## Situation, Authority, Purpose

- **Situation:** The situation should be a brief summary of the current environment. Some detail can be included in appendixes to the plan such as contact information and systems inventories. This is all part of "know your community."
- **Purpose:** The purpose outlines the reasons the plan was developed. This section will include background, purpose, and goals.

    Questions to ask when developing this section include:
    - ο What is the background of alerting in the jurisdiction?
    - ο Why is this plan needed?
    - ο What are the goals of this plan?
- **Goals:** The goals section describes what the plan is expected to accomplish in general terms.
- **Objectives:** The objectives section define the way that the goals will be accomplished.

## Alerting Plan Detail

The plan detail is the main section of the document. This section will vary widely from community to community. This section contains the details of who, what, and when IPAWS is used in the jurisdiction. The following information can be used to develop this section:
- What criteria are used to determine when to send an alert?
- What types of messages are permitted?
- What are the training requirements?
- What tools are to be used?
- What are the system security requirements?
- When and what can be tested and how?
- What coordination or outreach to the public and media is permitted?
- What is the process to activate alerts?

## Roles and Responsibilities

The roles and responsibilities of each level of jurisdiction are described and/or defined, including the following:
- Each level of jurisdiction
- Roles of each jurisdiction
- Responsibilities of each jurisdiction

- Restrictions of each jurisdiction

One of the major responsibilities is the review and maintenance of the plan. There should be a section describing the process used to keep the plan current, including the following information:
- How often the plan is reviewed
- Who has responsibility for reviewing
- How an entity submits changes

### Appendices

Appendices should contain additional information that is relevant to the plan or that may be needed for the plan, including other plans that may be relevant to IPAWS. Appendices can include the following:
- A table of acronyms and glossary
- Descriptions of the architecture of the alerting systems in the jurisdiction
    - Types of alerting systems used to generate alerts
    - Type of systems used to disseminate messages to the public
    - Detailed method for distributing wireless system messages
- Alert and notification capabilities—list all broadcasters, wireless providers, and other capabilities to provide alert and notification in the jurisdiction
- Example or sample messages and templates
- IPAWS application procedures
- Statewide EAS plan
- MOU from NWS for use of NWS radio for civil emergencies
- MOU from transportation agency for access to highway signs for IPAWS

If the plan is large and given the nature of the technology-centered systems for which the plan is in place, an acronyms list and glossary should be included. This section(s) lists acronyms and terms used in the plan, can be a single section or split into two separate sections, and can be an appendix or go before the appendixes.

## 3.4.    SHARED USE AND MEMORANDUMS OF UNDERSTANDING

### 3.4.1.    *Overview*

#### Background

IPAWS was developed primarily to provide a national system for presidential messages, but the system is available to State, local, and tribal entities. The current rules provide access to IPAWS at the county level. Many large cities, which do not represent entire geographical counties, also benefit from access. In addition, many incidents, such as a flood or wildland fire, extend beyond a single county or jurisdiction. Jurisdictions can also share resources and provide alerting for other jurisdictions. An MOU provides these abilities to the jurisdiction.

### Purpose

An MOU template has been created as a tool for States and counties to develop agreements with neighboring jurisdictions for the purpose of using IPAWS to notify the public of emergency incidents and protective actions.

This template can be modified in any way to address local situations to provide the best service to the public and responders.

An MOU should be developed for each county or entity that is an approved COG with IPAWS. This will allow the IPAWS PMO to correctly set up the permissions for the COG in IPAWS-OPEN.

### References

- Writing Guide for a Memorandum of Understanding (MOU) by SAFECOM
- Appendix F – Model MOU template
- IPAWS Rules of Behavior
- Code of Federal Regulations (CFR) 47 Part 11 — Emergency Alert System
- CFR 47 Part 10 — Commercial Mobile Alert System

### 3.4.2. MOU Components

### Introduction

The Introduction section describes the reason for the MOU and will serve as a background of the situation that leads to the development of the MOU. The introduction is intended to provide a high-level summary of the MOU. The following questions can guide the development of the introduction:
- Why is this MOU being created, what is the need being addressed, and what is the background?
- What agencies are participating in the MOU?
- Why is this MOU necessary?
- What agreements are set forth by this MOU?

### Purpose

The Purpose section should be a concise statement of the intention of the MOU. It explains how the agencies involved will use the MOU and under what circumstances. The following questions can guide the development of the purpose:
- When will it be used?
- How will it be used?

### Scope

The Scope section describes the specific extent of the MOU. It lists the agencies and jurisdictions included in the agreement and describes their relationship. The following can guide development of this section:

- Contact information for all parties
- List of FIPS codes of the entity
- List of authorized event codes allowed by the entity
- Specify when the MOU is in effect
- Description of the limits to using the system
- For local users, description of what is needed for State approval

### Definitions

The Definitions section describes the terms and acronyms used in the MOU and for the operation of the systems of the MOU where coordination is required.

### Policy

The Policy section describes the operation of IPAWS to which the MOU is agreeing. This is a high-level description of the intent and operation of the systems. The following questions can guide development of this section:

- Who can use the system?
- What is permitted to be done on the system?
- Which event codes can be used?

### Procedures

The Procedures section describes in detail the steps each participant takes to operate in compliance with the policy. This is detailed in step-by-step instructions.

### Changes to MOU

The Updates section describes the process of maintaining the MOU over the period of the agreement. The following questions can guide the development of the Updates section:

- How can the MOU be modified?
- How can the MOU be cancelled?
- If only one party of an MOU between three of more parties wants to cancel, what happens to the MOU?

Appendix F contains an example MOU as a reference.

## 4.  ALERTING TECHNOLOGIES SELECTION

*"Our Age of Anxiety is, in great part, the result of trying to do today's job with yesterday's tools..."*

*Marshall McLuhan*

### References

➢ Developing and Maintaining Emergency Operations Plans, Comprehensive Preparedness Guide (CPG) 101, Version 2.0, November 2010
➢ Local Emergency Operations Plan
➢ FEMA IS-2001 Threat and Hazard Identification and Risk Assessment (THIRA) Course
➢ Census Data at: https://www.census.gov/

### 4.1.  ALERT AND NOTIFICATION SYSTEM SELECTION CONSIDERATIONS

The selection of alert and notification systems should be based on information gathered during the planning process. Risks and community information will drive the alert and notification systems that are needed. In most cases, this will be a group of tools and systems that are used to notify various audiences.

Another consideration when selecting an alerting tool is whether a physical system or a hosted solution best meets needs. Both options are effective, but will not work for all agencies. For example, within the CSEPP community, a few counties were interconnected to physical radio transmitters to deliver alerts to the public. A hosted solution was not able to be interconnected to these radios.

Some advantages and disadvantages of hosted and physical systems are listed in the table below.

| | Advantages | Disadvantages |
|---|---|---|
| **Hosted** | • Maintained by hosting provider<br>• Accessible from almost anywhere<br>• Low capital costs | • Controlled by third party<br>• Requires Internet or other access<br>• High operational costs |
| **Physical System (Hardware)** | • Can be interconnected to other systems (e.g., radios)<br>• Controlled by agency<br>• Low operational costs | • Requires maintenance by agency staff<br>• System redundancy can increase costs<br>• High capital costs |

Whenever a system is selected, discussions should be had regarding its purpose and how the system can be measured to determine its effectiveness. Various systems have different target audiences; as

such, a variety of measures will need to be place to determine the effectiveness of alert and notification messages.

## 4.2.    IPAWS SYSTEM CONSIDERATIONS

The CSEPP communities have unique alerting needs due to the congressional mandate to provide "maximum protection" to the public. To improve system confidence and to achieve better information on how IPAWS functions, testing was planned and a test plan developed. Testing of CSEPP's use of IPAWS was executed on December 8 and 9, 2014. Information on the systems used by the participating sites as well as how IPAWS processes the messages was collected. Some issues encountered during testing are described below[4] and should be given consideration when selecting an alert and notification system.

- Applications took the time from the local device, not a network source. This resulted in several message failures, as the times of the CAP message were outside the allowable parameters of IPAWS-OPEN. The device time was changed and the issue was resolved.
- The use of default settings, including default end-dates, durations, and text from previous messages, was an issue. Some systems kept text from the previous messages and prepopulated a message. This resulted in duplicate messages or messages with a duration of 23 hours during testing. Users must carefully review each element.
- The issues with cutting and pasting text into the IPAWS applications were identified in pre-testing preparation. In the preparation phase, a test found that bullets were not acceptable characters. During testing, it was found that other formatting issues in some word-processing programs may affect the message text. Using a text editor to remove special format and characters worked in some cases, but caution should be used, as some web browsers may add formatting to the text that is not visible to the user.
- Some systems are designed to generate a message for only one distribution channel at a time. To test all channels, a message for each channel had to be created by the user.
- A major issue was the ability to cancel or update a message. Only two of the four systems tested provided the ability to cancel or update a message. A third vendor had this feature in beta testing and said that the cancel could be performed by editing the CAP message in an editing module. This was labor-intensive, required technical knowledge of the CAP format, and was not able to be done in an actual message by a typical user.

The interface that the system operator will use can also impact the system selected. Some advantages and disadvantages of simple and complex user interfaces are listed in the table below.

---

[4] The complete test report can be found at www.cseppportal.net.

| | Advantages | Disadvantages |
|---|---|---|
| **Simple Interface** | • Easy for users to create messages<br>• Pre-populated fields<br>• Less system knowledge needed to use application<br>• Easier to train users<br>• Less risk of errant alerts | • Fewer functions available to the user<br>• Limited availability of log files<br>• Troubleshooting available to the user may be limited |
| **Complex Interface** | • Many functions available to the user<br>• Detailed logs containing messages sent and responses are available to the user for troubleshooting | • Requires more training<br>• Difficult to operate (many fields or pages)<br>• Users need to understand the application as well as the operation of IPAWS and legacy EAS<br>• High risk for errant alerts |

The following suggestions for vendors arose during the after-action review:
- The system(s) should be able to do the following:
  - ο Synchronize time from a master clock or IPAWS-OPEN and not the user's device to ensure the times attached to messages are valid
  - ο Provide validation of polygons for IPAWS and the distribution channel before they are sent to IPAWS-OPEN
  - ο Provide text validation to ensure that there are no improper or invisible characters in the message text
  - ο Include a message cancel and/or update function
  - ο Allow users to see the message status without having to refresh the page
  - ο Eliminate the need to create the same message for each dissemination pathway
  - ο Allow the user to retry a message to a failed path when posting a message failed with HTTP errors (e.g., 503 service temporarily unavailable)
- Easier to understand user manuals, job aids, and refresher training should be developed

These items should also be given consideration when selecting an alert and notification system.

## 4.3. FUNCTIONAL REQUIREMENTS

A functional requirement is a statement of a specific function that a system or device must or should do. Functional requirements are used for various reasons, including the following:
- Developing a new device or system
- Testing a device or system
- Procuring a device or system

Functional requirements should be developed based on intended or expected functions that the authority needs. These requirements are based on the risks, populations, goals, and objectives developed above. To be effective, these requirements should have the following attributes:

- **Clear:** Each requirement should be a single complete action or function, and the reader should be able to draw only one interpretation of it. Other readers of the requirement should arrive at the same interpretation. Subjective words like *user-friendly, easy, simple, rapid, efficient, several, state-of-the-art, improved, maximize*, and *minimize* should be avoided. Requirements should use simple, straightforward language and not jargon or slang.
- **Verifiable:** Devise tests or use other verification approaches, such as inspection or demonstration, to determine whether each requirement is properly implemented in the product. If a requirement is not verifiable, determining whether it was correctly implemented is a matter of opinion. Requirements that are not consistent, feasible, or unambiguous also are not verifiable. Any requirement that says the product shall "support" something is not verifiable.
- **Feasible:** It must be possible to implement each requirement within the known capabilities and limitations of the system and its environment. To avoid infeasible requirements, have a developer work with the requirements analysts or marketing personnel throughout the elicitation process. This developer can provide a reality check on what can and cannot be done technically, and what can be done only at excessive cost or with other tradeoffs.
- **Necessary:** Each requirement should document something the customers really need or something that is required for conformance to an external requirement, an external interface, or a standard. Another way to think of *necessary* is that each requirement originated from a source you recognize as having the authority to specify requirements. Trace each requirement back to its origin, such as a use case, system requirement, regulation, or some other voice-of-the-customer input. If you cannot identify the origin, perhaps the requirement is an example of "gold plating" and is not really necessary.

Appendix B contains an example requirements document.

## 4.4. PROCUREMENT METHODS

Once the specifications of the functions needed are determined, there may be a need to procure one or multiple systems. It is important to follow the procurement requirements of your agency. These systems can be capital expenditures for fixed equipment or operational expenditures for maintenance or a service.

Some of the methods to procure systems are in the following table:

| Method | Use |
|---|---|
| Request for Proposals (RFP) | An RFP will usually allow for an assessment of a proposed solution in a holistic approach. This allows the entity to review the best solution for its needs and not rely solely on price. This method is best for complex systems with multiple different solutions, components, or options. |
| Request (or Invitation) for Bid (RFB or ITB) | An ITB will usually require the entity to select the lowest cost proposal. This is used for procurement of items that are commodities rather than complex systems. This is best for items that can be very clearly defined. |

| Method | Use |
|---|---|
| Series of proposals | Pre-identifying a series of vendors that offer the solution and requesting proposals from these is allowed in some jurisdictions. This is usually used for lower-cost solutions. Many jurisdictions place a maximum value where this can be used. This is best for non-complex systems or components. |
| Direct procurement | Direct procurement is allowed in some jurisdictions. This is used when an entity has a clear idea of the solution. Caution must be used with this method to make sure this solution will meet the needs. This is best used when there are clear specifications and the solution meets the specifications. |

## 4.5.  CALCULATING COST OF OWNERSHIP TO DETERMINE SUSTAINABILITY

Many local governments and public safety agencies use Federal grant funds to implement technology that aligns with short- and long-range planning goals to the benefit of their constituents. During a time when most local governments face budget cuts, grant funding often provides needed resources. A recurring question is: What happens when grant funding ends? Many agencies do not fully realize the total costs of ownership and may find it difficult to sustain the investment already made or to budget appropriately.

Examining the total cost of ownership and an entity's ability to sustain a system when funding ends is imperative. Total cost of ownership, simply put, is a financial estimate whose purpose is to help consumers determine direct and indirect costs of a system or product. Sustainability has multiple meanings, but for this purpose means "the ability to maintain or support."

Total cost of ownership attempts to measure the financial impact of implementing a technology over its life cycle, which may be 5 years or more. It will also be necessary to include a percentage for cost increases. For example, there may be an initial cost, monthly or annual maintenance, connectivity, database maintenance, and interface costs to add IPAWS to an existing emergency notification system.

To determine the total cost of ownership, the steps below should be followed.

**Step 1: Identify the costs of the of the solution**
- What are the one-time costs (equipment, software, or connectivity)?
- What are the recurring costs (licenses fees, services, maintenance)?

In the example above (i.e., adding IPAWS to an existing emergency notification system), the following one-time and recurring costs were identified. (Note: costs used in the simplified example below are not actual and are used strictly to show calculations; numbers are rounded to the nearest dollar when necessary.)

| | Cost | One-Time | Recurrence |
|---|---|---|---|
| Initial equipment cost | $35,000 | ✓ | |
| Non-recurring network expense | $600 | ✓ | |
| Monthly charge | $1,200 | | Monthly |
| Annual maintenance | $13,200 | | Annually |
| Interface | $1,000 | | Monthly |
| Database maintenance | $500 | | Monthly |

When calculating total costs, there are numerous aspects to consider, including the following:

- Technology
  - o Network, server and workstation hardware and software
  - o Installation and integration or migration
  - o Maintenance
  - o Warranties
  - o Operating system and specialized licenses
  - o License compliance
  - o Upgrades and patches
- Operations
  - o Monthly recurring costs
  - o Personnel (IT, management)
  - o Training
  - o Backup and recovery processes
  - o Security (breaches, recovery and prevention)
  - o Downtime
  - o Electricity (equipment, cooling, backup)
  - o Infrastructure
- Long-term
  - o Replacement
  - o Future upgrade or scalability

**Step 2: Determine the lifetime of the solution**
- What is the life span of the solution?
- What is the expected timeframe the solution will be needed?
- What is the expected inflation rate of costs?

Will the solution last 5 years, 10 years, or 20 years? Is the solution temporary and only needed for 18 months? What is the anticipated inflation rate? Is inflation increasing or decreasing?

Historical inflation data from 1914 to the present may be found at the following website:
http://www.inflationdata.com/inflation/inflation_rate/historicalinflation.aspx

**Step 3: Calculate recurring costs for Year 1**
The recurring costs identified in step 1 are multiplied by their recurrence to determine the recurring costs for Year 1. Monthly is multiplied by 12, semi-annually is multiplied by 2, and annually is multiplied by 1.

|  | Cost | Recurrence | Calculation | Total for Year 1 |
|---|---|---|---|---|
| Monthly charge | $1,200 | Monthly | $1,200 × 12 | $14,400 |
| Annual maintenance | $13,200 | Annually | $13,200 × 1 | $13,200 |
| Interface | $1,000 | Monthly | $1,000 × 12 | $12,000 |
| Database maintenance | $500 | Monthly | $500 × 12 | $6,000 |

**Total Recurring Costs  $45,600**

**Step 4: Calculate recurring costs for remaining years of solution**
For example, if the life span of the solution is 5 years and a 2-percent inflation rate is anticipated, recurring costs will need to be calculated for years 2–5 taking into account the inflation rate.

As shown above, the costs that recur over the life cycle of the equipment are the monthly charge, annual maintenance, interface, and database maintenance.

To calculate a percentage increase of 2 percent (or .02), for example, the annual total of the respective category is multiplied by 1.02 or 102 percent. Both yield the same result.

$$\$14,400 \times 1.02 = \$14,688$$

$$\$14,400 \times 1025 = \$14,688$$

In this example, monthly charges for Year 2 would total $14,688.

The process is repeated for Year 3 using the total for Year 2 as the starting point as Year 3 would see an anticipated 2 percent inflation rate over Year 2.

$$\$14,688 \times 1.02 = \$14,982$$

$$\$14,688 \times 102\% = \$14,982$$

Years 4 and 5 are calculated in the same manner. This process is repeated for each recurring charge. If the solution has a longer life span, the calculations are repeated for each remaining year of the solution. A solution with a longer life span may require upgrades, which would increase costs for the respective year.

The table below depicts the recurring costs over 5 years.

|  | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Total |
|---|---|---|---|---|---|---|
| Monthly charge (annual totals) | $14,400 | $14,982 | $15,282 | $15,588 | $15,900 | **$76,152** |
| Annual maintenance | $13,200 | $13,464 | $13,733 | $14,008 | $14,288 | **$68,693** |
| Interface (annual totals) | $12,000 | $12,240 | $12,485 | $12,735 | $12,990 | **$62,450** |
| Database Maintenance (annual totals) | $6,000 | $6,120 | $6,242 | $6,367 | $6,494 | **$31,223** |

**Total Recurring Costs   $238,518**

To calculate a decrease in the inflation rate, the percentage of decrease is subtracted from 1.0 or 100 percent, and that result is multiplied by the annual total. For example, a decrease of ½ percent (or .005) would be .995 or 99.5 percent. Both yield the same result.

$$\$14,400 \times .995 = \$14,328$$

$$\$14,400 \times .99.5\% = \$14,328$$

In this example, monthly charges for Year 2 would total $14,328.

**Step 5: Calculate total cost of ownership**
The recurring costs are added to the one-time costs to determine total cost of ownership. In this case, the two one-time costs are the initial equipment cost and the non-recurring network expense.

The table below depicts the total cost of ownership for a solution with a 5-year life cycle and an anticipated 2 percent inflation rate.

|  | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Total |
|---|---|---|---|---|---|---|
| Initial Equipment Cost | $35,000 | $0 | $0 | $0 | $0 | **$35,000** |
| Non-recurring network expense | $600 | $0 | $0 | $0 | $0 | **$600** |
| Monthly charge (annual totals) | $14,400 | $14,982 | $15,282 | $15,588 | $15,900 | **$76,152** |
| Annual maintenance | $13,200 | $13,464 | $13,733 | $14,008 | $14,288 | **$68,693** |
| Interface (annual totals) | $12,000 | $12,240 | $12,485 | $12,735 | $12,990 | **$62,450** |
| Database Maintenance (annual totals) | $6,000 | $6,120 | $6,242 | $6,367 | $6,494 | **$31,223** |
| **Yearly Totals** | $81,200 | $46,806 | $47,742 | $48,698 | $49,672 | |

**Total Cost of Ownership   $274,118**

As indicated in the table above, the total cost of ownership in this example is more than $270,000. This does not include the costs for any upgrades that may be necessary over the 5 years.

It is important to note that planning should take place for either the upgrade or replacement no later than Year 4. Initial planning for large capital costs should begin as early as Year 2 in a 5-year replacement cycle.

If a comparison is necessary for costs of existing systems versus proposed ones, give consideration to the costs required to maintain the existing system that may not necessarily be required for the one proposed. For example, many applications are now web-based, which alleviates the need for hardware and software purchases.

The steps listed above can also be used to compare costs if multiple solutions are available or offered. This is especially important if initial costs appear similar; recurring costs may vary greatly between solutions over their respective life spans, particularly in terms of licenses.

Determining an entity's ability to sustain technology funded initially through a grant does not need to be overwhelming but does require a comprehensive review of all aspects to ensure no costs are overlooked.

## 5. COG STATUS

*"Permit no hour to go by without it due improvement."*

*Thomas Kempis*

**References**

➢ IPAWS Toolkit for Alerting Authorities
➢ FEMA IS-247a - Integrated Public Alert and Warning System (IPAWS)
➢ FEMA IS-251 – Integrated Public Alert and Warning System for Alerting Authorities
➢ http://www.fema.gov/how-sign-ipaws

IPAWS is a powerful tool for local alerting authorities to inform the public. IPAWS allows the authority to create a single message and distribute through multiple channels. To request access to IPAWS, the alerting authority needs to follow a few easy steps, which are shown on the following page.

**1. Select IPAWS compatible software**

Software should be successfully tested in an IPAWS OPEN test environment. Refer to IPAWS OPEN Developers (http://www.fema.gov/private-sector-0#psdevelopers) for approved vendors.

**2. Apply for a Memorandum of Agreement with FEMA**

Download the IPAWS Memorandum of Agreement (MOA) from http://www.fema.gov/library/viewRecord.do?id=6019, review the instructions, complete and scan. PLEASE e-mail the scanned application directly to FEMA at ipaws@dhs.gov. In the subject line of the e-mail, indicate "Operational COG Application. The FEMA MOA Coordinator will prepare and return the MOA for signature after it is submitted.

**3. Apply for public alerting permissions**

Once your MOA has been initially approved by the FEMA MOA Coordinator and your selected IPAWS OPEN Developer has indicated they are capable of sending public alerts, the FEMA MOA Coordinator will e-mail you an application for PUBLIC ALERTING PERMISSION. You may complete and send to: ipaws@dhs.gov and your State coordinator

Alerting authorities (local jurisdictions) must complete an application defining the types of alerts they intend to issue and the extent of their geographic warning area. The application for IPAWS PUBLIC ALERTING AUTHORITY will be provided when you apply for a COG MOA, along with contact information for a designated state coordinator.

**4. Complete IPAWS web-based training: IS-247 Integrated Public Alert and Warning System. Link to the overview and course is:**

The course should take approximately 2 hours to complete and is a prerequisite for full access to IPAWS OPEN for the purpose of public alerting. Upon completion, please send a copy of the course completion certificate to FEMA at ipaws@dhs.gov and the state coordinator

## 5.1.    SELECT IPAWS-COMPATIBLE SOFTWARE

Prior to applying for IPAWS authorization, the alerting authority must select compatible software to generate CAP messages. This is the only cost for IPAWS the alerting authority will have. FEMA IPAWS and the distribution channels do not charge a fee to alerting authorities.

It is important to identify the alerting authority's needs and requirements before selecting software. Information on the development of specifications, cost basis, and procurement is in Section 4, Select Alerting Technologies.

The chosen software must be compatible with IPAWS-OPEN and provide the capabilities that your organization requires. For a list of private-sector developers who have access to IPAWS-OPEN, please view the list of IPAWS-OPEN developers at http://www.fema.gov/how-sign-ipaws.

## 5.2.    APPLY FOR MOA

Who can sign up for IPAWS?
- Federal agencies
- State government organizations
- Local government or public safety organizations

A Federal, State, or local alerting authority that applies for authorization to use IPAWS is designated by IPAWS as a **Collaborative Operating Group (COG).**

The alerting authority should start by visiting the FEMA IPAWS website and viewing a short 5-minute video and review the most current IPAWS Toolkit on IPAWS before beginning the process of implementing IPAWS in your jurisdiction. The link is below:

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

The IPAWS website also has the current application form to use. This application requests information on the agency and contact information on key agency personnel. It is important for the agency to list the system(s) it will use to compose and send alerts to IPAWS. The application has room for more than one system for those that may require multiple systems.

The application should be e-mailed directly to FEMA at ipaws@fema.dhs.gov. Please indicate "COG Application" in the subject line of the e-mail.

When a local alerting authority submits the application for an MOA, it should notify the State IPAWS coordinator. The State coordinator may be able to assist in preparation of the application.

## 5.3. APPLY FOR PERMISSIONS

The COG coordinator at IPAWS PMO will process the application for an MOA. IPAWS will send several documents for the alerting agency to complete. These forms are required to be completed by the local alerting authority and reviewed and approved by the State.

**MOA:** The MOA is the actual agreement between IPAWS and the alerting authority. The majority of the information in this document, including Rules of Behavior, comes from the application. The alerting authority should review this information carefully. Some authorities use parts of this document and the Rules of Behavior to train and ensure each authorized user of the system fully understands the operation of IPAWS.

**Application for IPAWS Public Alerting Authority:** This document is completed by the alerting authority. This form is used to identify the distribution channels the authority would like access to and the specific message incident types.

Distribution channels for alerting are:
- CAPEXCH: alerts from COG to COG
- EAS: alerts to broadcasters
- WEA: alerts to cell phones
- NWEM: alerts to weather radios
    - In addition to signing up for IPAWS, operational NWEM capability requires additional COG level permissions from NWS
- PUBLIC: alerts to public with Non-EAS PUBLIC alerts
    - PUBLIC alert messages can be retrieved using IPAWS All-Hazards Information Feed
    - PUBLIC alert messages can be retrieved using "getMessageList" method within 24 hours as default retrieval configurable time period value

This application must be signed by the designated state official. After completing this form, it should be forwarded to the state coordinator for approval and then forwarded to IPAWS PMO.

## 5.4. COMPLETE REQUIRED TRAINING

Each person who will generate IPAWS messages should have completed the FEMA Independent Study course FEMA IS-247a – "Integrated Public Alert and Warning System (IPAWS)." This course is required after applying for an MOA and permissions, but this course may be helpful prior to the application and selecting a system. This course is available online at the following link:

http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-247.a

The goal of this course is to provide authorized public safety officials with the following:
- Increased awareness of the benefits of using IPAWS for effective public warnings
- Skills to draft appropriate, effective, and accessible warning messages

- Best practices in the effective use of CAP to reach all members of their communities

The course takes approximately 2 hours to complete and is a prerequisite for full access to IPAWS-OPEN for the purpose of public alerting. FEMA does not provide training on third-party authoring software. Respective vendors should be contacted for any software support questions.

Copies of the course completion certificates for the alerting authority must be sent to your State coordinator and the IPAWS PMO before the authority will be activated. All authorized staff should also have training on the specific equipment and procedures and review and sign a copy of the Rules of Behavior. Records of all training should be developed and maintained. Section 6.2, Training, has additional information on training and documentation.

## 5.5.  COG ID ISSUED

Once all forms have been completed, signed, and State-approved, IPAWS will issue the COG identification and digital certificate. The COG will get several communications from FEMA that include the COG ID, certificate, and passwords. The digital certificate is good for 3 years. The IPAWS PMO will reissue certificates as needed. The certificate should be added to the selected IPAWS system. Coordinating with the vendor or service provider will usually make this easier.

IPAWS has also begun to issue a TEST COG ID and Certificate. If the selected IPAWS system can accept two or more IDs, this test certificate should be added. The test COG allows the authority to send test messages to the IPAWS Test Lab at the Joint Interoperability Test Command (JITC). This will provide the capability to practice and train staff on the system.

## 5.6.  APPLY FOR NWEM PERMISSION

If the alert authority requested permission to send messages to the NOAA weather channel, the alert authority must apply for additional authority from NWS. The NWEM channel provides access to NWS radio. The NOAA website describes the system.

> *HazCollect, the NWS's All-Hazards Emergency Message Collection System, is a comprehensive national solution for the centralized collection and efficient distribution of Non-Weather Emergency Messages (NWEMs). NWEMs created by government officials with public warning authority are distributed through the NWS dissemination infrastructure, NOAA Weather Radio All Hazards, other national systems, and to the nation's Emergency Alert System (EAS).*
>
> *A NWEM is a specialized form of an OASIS Common Alerting Protocol (CAP) alert. The CAP alert is sent to the HazCollect service via FEMA's Open Platform for Emergency Networks (IPAWS-OPEN) interoperability infrastructure.*[5]

---

[5] National Weather Service. 2013. "HazCollect." Accessed online September 28, 2015. http://www.nws.noaa.gov/os/hazcollect/

For more information, refer to: http://weather.gov/os/hazcollect.

To apply for access, the application must be completed online at:
https://ocwws.weather.gov/cog/login.php.

To complete this application, the authority must have its approved COG ID.

## 6. IPAWS USE

*"Knowledge is of no value unless you put it into practice."*

*Anton Chekhov*

**References**

➢ Alert and Notification Plan
➢ FEMA IS-247a - Integrated Public Alert and Warning System (IPAWS)
➢ FEMA IS-248 - Integrated Public Alert and Warning System (IPAWS) for the American Public
➢ Code of Federal Regulations (CFR) 47 Part 11 — EMERGENCY ALERT SYSTEM
➢ CFR 47 PART 10 — COMMERCIAL MOBILE ALERT SYSTEM
➢ Common Alerting Protocol. "v. 1.1, OASIS Standard CAP-V1. 1." (2005).
➢ Common Alerting Protocol, v. 1.2 USA Integrated Public Alert and Warning System Profile Version 1.0. (2009).
➢ National Weather Service, Operations and Services; Public Weather Services, NWSPD 10-5, Non-Weather Related Emergency Products Specification (Instruction 10-518, July 28, 2010)

The use of IPAWS and other alert and notification systems will follow the same preparedness cycle as any other system or process in emergency management.[6]



- Plan
- Organize and Equip
- Train
- Exercise
- Evaluate and Improve

The plan has been developed. The "organize and equip" component of the cycle will require documentation of how to use the systems.

---

[6] Federal Emergency Management Agency. 2010. *Developing and maintaining emergency operations plans*: *Comprehensive Preparedness Guide 101,* version 2.0.

## 6.1. POLICIES, PROCEDURES, AND GUIDELINES DEVELOPMENT

### 6.1.1. Overview

To effectively use IPAWS and other alert and notification systems, there should be written documentation on the use of these systems. The alerting authority should develop documentation of user actions to provide the critical public alerts and notifications that are needed and expected by the public.

Each governmental agency has different structures and the name of this documentation will vary between agencies. The terms *standard operating procedures (SOPs), policy,* and *guidelines* and other terms may have additional impacts to the documents. An agency should always review the documentation with the appropriate legal and alerting authorities.

**Policy:** A policy is generally considered a firm rule that must be followed. Merriam-Webster defines *policy* as "a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions."[7] Policies may have other specific meanings based on governmental structure. Policies can often only be approved by an elected official in a governmental entity. Policies cover specific situations and can often restrict the actions of staff in an emergency.

**Procedure:** A procedure is often used to define the steps a person should take in a specific situation. Merriam-Webster defines *procedure* as "a series of actions that are done in a certain way or order: an established or accepted way of doing something."[8] Procedures are generally developed by management as instructions to staff. Procedures list specific actions and may restrict the actions of staff in an emergency.

**Guideline:** A guideline is often used to describe a general course of action. Dictionary.com defines *guideline* as "any guide or indication of a future course of action."[9] Guidelines are generally used to provide direction to a trained person. A guideline can allow a trained person to apply personal knowledge and training to an emergency using the provided guidelines to determine the specific actions needed.

Regardless of the name used for these documents, they need to include the information and actions needed to successfully alert and notify the public of emergencies and dangers. These operational documents should cover the following questions:
- Who can send alerts?
- What is the authority?
- How is authority delegated?
- Who can request an alert be issued?

---

[7] http://www.merriam-webster.com/dictionary/policy
[8] http://www.merriam-webster.com/dictionary/procedures
[9] http://dictionary.reference.com/browse/guideline

- When can an alert be issued?
- What systems should be used?
  - EAS
  - WEA
  - NWS
  - IPAWS All-Hazards Feed
  - ENS
  - Sirens
  - Other systems
- How are the systems operated?
- What segment of the populations does each system reach?
- Can multiple systems be used simultaneously to reach more people?
- What follow up from an alert is needed?
- What is the typical public reaction? (Call 9-1-1, ignore, etc.)
- What is the desired public reaction?
- Who needs to be notified before or after alerts?
  - 9-1-1
  - Public Information Office (PIO)
  - Alert Authority
  - Other COGs
  - State
  - Tribe
- How often and when is the alert re-sent?
- How are the systems used for exercises and pre-planned events?
- Does your alerting tool support IPAWS in a live environment as well as support a test environment with the IPAWS Lab?

### 6.1.2.  Documentation Process

The process to develop operational documentation follows a simple order similar to the emergency management preparedness cycle.

1. Develop
2. Publish
3. Use
4. Review and Update

#### Develop

The first step in developing operational documents is to identify a team to work on the documentation. This team should consist of the staff that operates these systems, management, local broadcasters, and even the public in some cases. Consider a member of the public in jurisdictions that may have unique audiences like people with disabilities and others with access and functional needs or those with cultural differences.

The next step is research. Time should be spent researching the information needed to effectively alert the public. A partial list of documents to review is as follows:

- Local Alert Plan
- Local Emergency Operations Plan
- State Alert Plans
- State EAS Plans
- FEMA IPAWS Rules of Behavior
- FCC Rules (47 Code of Federal Regulations [CFR] 10 and 47 CFR 11)
- FCC CSRIC IV Best Practices for alerting and security
- Vendor provided instructions and training
- Lessons Learned from previous events and exercises

The team should ask two questions: What documents are needed? What format should these documents be in?

The team will determine what documentation is needed based on the research. This can be an assortment of different documents such as a policy on who can send alerts, a job aid, or a checklist for the system operator. The team will then outline the various documents and assign an editor and/or writer to each document or sections.

The document text is developed and shared within the team. The sharing of document drafts among team members will help assure the documents complement each other and do not conflict. The team should develop an internal review process to assure the documents are developed into a comprehensive guide.

The draft documents should be reviewed; some of the people to consider using to review drafts are as follows:

- System users: System users can review text to see if the language is easy to follow. The best reviewers are a combination of those with limited or no knowledge of the system and ones with good knowledge of the system. This allows for both perspectives.
- PIO: The PIO can review text to assure that the use of the system(s) is in line with the public information needs of the community.
- Alert authority: The alert authority should review the documents and possibly provide approval. This is best when the authority is delegated.
- Legal representative: Documents should be reviewed by the jurisdiction's legal counsel to provide protection for the jurisdiction.

### Publish

It is recommended that the documents be published in two steps.
- Draft—for exercise use only

- Final—for pilot test, etc.

The terms used to refer to these are less important than the process. A first-reviewed document is placed into limited use. This use can be for an exercise or a special event. This may follow the Homeland Security Exercise and Evaluation Program (HSEEP) process and start with a tabletop exercise and build from there, followed by review and updates as needed. This process will make the final document better.

The final approved document should be published. This document should be available to all stakeholders involved in its creation. Most importantly, it needs to be published to the users and then incorporated into user training.

### Use

The first most important part of the use of any technology and process is the training. The technology and operational documents should be used to train all users to ensure they understand their roles, responsibilities, and actions required to perform their functions. Many agencies have initial training and then move on to the next issue. Training is improved when it is ongoing and includes refresher sessions. It is best when the system and process are integrated into daily or regular activities. (Refer to Section 6.2, Training, for more information.)

One of the best ways to maintain skills is to integrate actions into regular work flows. Public alerting may not lend itself to daily use but would fit into an agency's regular exercise schedule. IPAWS and other alerting tools may be used in exercises and more routine public notifications. IPAWS has been used for boil-water notices, notifications to stay off roads during winter storms, 9-1-1 outages, and to disregard accidental siren activations. The Model Alert and Notification Plan (Appendix F) and Section 6.3.2, Pre-planned Events, contain information on the use of IPAWS for pre-planned events. Section 6.3.3, Exercise, contains additional information on the use of alerting systems. Any use should meet applicable laws and the State's and jurisdiction's alerting plans.

An agency should also have a formal feedback process in place to elicit comments and suggestions for changes, modifications and improvements to technology and processes. This feedback is used to review and update the documents.

### Review and Update

Each procedure, plan, and technology should be reviewed and updated as risks and situations change. Feedback from users, incidents, exercises, and vendors allows these documents to be improved over time. After each major exercise or incident, the response should be reviewed for lessons learned and places to improve. At a minimum, all policies, procedures, guidelines, plans, and systems should be reviewed annually.

One method to accomplish this is to segment systems in use into four or six groups. One group can be reviewed quarterly or bimonthly, making the process manageable. Documents should include a history table noting when it was published, last updated, and last reviewed.

### 6.1.3. Documentation Content

Each document should contain basic information, and be structured to align with an agency's existing format. One format example is provided below.

**Header:** This contains the authority, title, effective date, revision number, and revision date.

**Purpose:** The purpose describes the need for the guideline and a summary of the guideline's intent.

**Scope:** The scope describes to whom and when the guideline applies.

**Guideline:** The guideline itself describes the steps to take or the reasons for or options for actions allowed.

Example guidelines are included in Appendix G, Model Alerting Guidelines.

## 6.2. TRAINING

All systems and procedures should be reinforced with training. *Training* is defined as "a process by which someone is taught the skills that are needed for an art, profession, or job"[10] or "to give the discipline and instruction, drill, practice, etc., designed to impart proficiency or efficiency."[11] To effectively use and perform the critical functions of alerting the public, all users must understand the systems and procedures. This is accomplished with two types of training—initial and recurring.

**Initial training** consists of training from the vendor on the basic and advanced operation of the system as well as operational procedures. This training is provided to all staff and users when a new system is deployed and for each new employee during new hire training.

**Recurring training** is provided periodically to refresh the skills and knowledge of the users. The use of the systems will determine how often this training is needed. All skills are perishable, which is why skills such as using a telecommunications device for the deaf (TDD) are practiced regularly. The more a skill is used, the longer that skill is maintained. All IPAWS training should include the use of the IPAWS Lab at JITC to provide feedback to the users. (Refer to Section 6.3.1, IPAWS Message Viewer, for more information.)

For IPAWS or any alert and notification system, users should have training on the following:
- Use of technology

---

[10] http://www.merriam-webster.com/dictionary/training
[11] http://dictionary.reference.com/browse/training

- Agency procedures for alerting
- Agency post-alert procedures
- Creating and formatting messages
- Security procedures for the technology

All training should be conducted in methods that correspond with the ways people learn, which has been discussed over the years. Traditionally three types of learning styles are used to reinforce skill development:
- Seeing; i.e., a visualizing style
- Hearing; i.e., an auditory style
- Doing; i.e., a tactile (kinesthetic) style

Another model breaks out seven learning styles, which are described as follows:

- Visual (spatial); i.e., a preference for using pictures, images, and spatial understanding
- Aural (auditory-musical); i.e., a preference for using sound and music
- Verbal (linguistic); i.e., a preference for using words, both in speech and writing
- Physical (kinesthetic); i.e., a preference for using your body, hands and sense of touch
- Logical (mathematical); i.e., a preference for using logic, reasoning and systems
- Social (interpersonal); i.e., a preference for learning in groups or with other people
- Solitary (intrapersonal); i.e., a preference for working alone and using self-study[12]

A good resource for training is FEMA's Independent Study Program *IS-265: Basic Instructional Skills* from the Emergency Management Institute (EMI) at http://training.fema.gov/. This course provides a basic understanding of the instructional and learning process.

An important component of any training is recordkeeping. Training records should include the trainer, the curriculum, and attendees. Results of tests, quizzes, or performance are also good to maintain in the training record. Local legal staff should be consulted to determine what level of information, open records impacts, and record retention issues may exist for your agency.

## 6.3.    EXERCISE AND REGULAR USE

CSEPP conducted a series of tests using participating counties' alert authoring tools and the IPAWS Lab at JITC. Some of the lessons learned that should be kept in mind as these tools are used are provided below.
- The tools used to author IPAWS messages should be selected based on the needs of a respective agency.
- All IPAWS tools should include simple ways to cancel or update messages.
- The public should be educated on IPAWS and the messages that can be sent.

---

[12] learning-styles-online.com. 2015. "Overview of learning styles." Accessed online September 28, 2015. http://www.learning-styles-online.com/overview/

- Not all cellular phones will display the same message the same way.
- Not all display systems and text-to-speech display messages the same way.
- Some text-to-speech will read "#" as "pound sign"; others will read it as "hashtag."
- Display systems do not recognize bullet points.
- Other characters used can change a message.
- Each authoring tool operates differently and can implement similar features differently.
- A user's ability to practice and test authoring tools will benefit deployment and operationalization of these systems.
- The more comfortable and confident users are with the systems, the more likely the systems will be used.
- All authoring tools should have complete and easy-to-understand user manuals and job aids.
- All authoring tool vendors should conduct hands-on user training (in person or webinar).
- More user interaction is needed with the vendors to ensure better tools.

To use alert and notification tools effectively, skills learned must be kept current. A skill not used is often forgotten. These skills can be used in regular operations, exercises, and pre-planned events.

### 6.3.1.　Regular Operations

Integrating alert and notification systems into regular operations can take some outside-the-box thinking. The benefits of integrating these systems are that it builds familiarity with systems, enables better thinking skills, and provides better response to emergencies. Use should include operation of the technology as well as forming messages and determining distribution channels. These activities will build skills. A variety of events can assure more use of the systems.

The first opportunity is during normal testing. Many systems require a weekly test. While not all distribution channels allow this, some do. By using IPAWS to send these required tests, users will gain experience with the systems and the distribution channels that allow tests can be used. These tests should be conducted at different times of the day and days of the week to allow multiple users to practice. Some systems allow users to set the tests to run automatically with little or no user intervention. When done in this manner, a great practice opportunity is lost.

Many agencies work with other governmental agencies such as highway, roads, water, sewer, or parking agencies. These relationships can be harnessed to provide users with additional messages to develop, the opportunity to select the appropriate distribution method, and to use the equipment to send alerts and notifications to the public.

Depending on the technology in use, there may be other opportunities to use the system(s). If the system(s) allows call groups, perhaps it is used for special unit call outs, announcements, overtime notifications, etc. Each agency will have its unique cases where alert and notification systems can be used within the rules, even for pre-planned events as described below.

### 6.3.2. Pre-planned Events

One way to exercise IPAWS in the organization is to use it for appropriate pre-planned events, such as drills, planned power outages, fairs, races, etc. This is allowable under the rules as long as the authority determines it is appropriate. During the planning of a pre-planned event (exercise or public event), the risks associated with the event should be identified. If the planned event has a potential risk to the public or public safety, the use of IPAWS to mitigate that risk may be appropriate. Appendix F, Model Alert and Notification Plan, has an appendix for the use of IPAWS for pre-planned events.

Examples of events and risks are provided below.

- Event: Controlled burn of large area
  Risks: Smoke on roadway impairing driving; aggravating medical conditions of people in area

- Event: school active-shooter exercise
  Risks: Panic of the general public in the area; Good Samaritan's reaction and putting the exercise players at risk

- Event: Major bicycle road race
  Risks: Traffic accidents; injury to riders and bystanders

IPAWS has several dissemination media. Each system has a different audience and rules for use.

| Dissemination System | Audience | Rules | Notes |
|---|---|---|---|
| Emergency Alerting System (EAS) | Broadcast radio and television viewers (not Internet or satellite) | 47 CFR 11 State EAS Plan | Broadcasters are not required to re-transmit alerts from local authorities. An EAS alert will be delivered to a large audience. |
| Wireless Emergency Alerts (WEA) | Wireless phones in the area of the alert | 47 CFR 10 | WEA has specific criteria for use. See * below. |
| Non-Weather Emergency Messages (NWEM) | Weather radio users | NWS policies | NWEM alerts will be sent to a National Weather Service (NWS) transmitter that covers a large area. The alert may also be rebroadcast by broadcast radio and television as an EAS message, but the entities are not required to carry. |
| IPAWS All Hazards Information Feed | Third-party software and service providers; usually a subscription type service | IPAWS rules | Currently, defining specific criteria for delivery due to the many varied systems using this data is unclear. |
| Collaborative Operating Group (COG) to COG | Other specific COGs | IPAWS rules | Used to coordinate and share information between COGs. |

\* For an alert to be sent to the WEA system, the event must meet the following criteria in accordance with 47 CFR 10.400:

> *(1) Urgency. The CAP Urgency element must be either Immediate (i.e., responsive action should be taken immediately) or Expected (i.e., responsive action should be taken soon, within the next hour).*

> *(2) Severity. The CAP Severity element must be either Extreme (i.e., an extraordinary threat to life or property) or Severe (i.e., a significant threat to life or property).*

> *(3) Certainty. The CAP Certainty element must be either Observed (i.e., determined to have occurred or to be ongoing) or Likely (i.e., has a probability of greater than 50 percent).*

When determining the event code to use, the following definitions of some common codes from the NWS Instruction 10-518 *Non-weather Related Emergency Products Specifications* are provided to assist in compiling the alert message.

> ***Civil Danger Warning (CDW).*** *A warning of an event that presents a danger to a significant civilian population. The CDW, which usually warns of a specific hazard and gives specific protective action, has a higher priority than the Local Area Emergency (LAE). Examples include contaminated water supply and imminent or imminent or in-progress military or terrorist attack. Public protective actions could include evacuation, shelter in place, or other actions (such as boiling contaminated water or seeking medical treatment).*

> ***Civil Emergency Message (CEM).*** *An emergency message regarding an in-progress or imminent significant threat(s) to public safety and/or property. The CEM is a higher priority message than the Local Area Emergency (LAE), but the hazard is less specific than the Civil Danger Warning (CDW).*

> ***Local Area Emergency (LAE).*** *An emergency message that defines an event that, by itself, does not pose a significant threat to public safety and/or property. However, the event could escalate, contribute to other more serious events, or disrupt critical public safety services. Instructions, other than public protective actions, may be provided by authorized officials. Examples include a disruption in water, electric or natural gas service, or a potential terrorist threat where the public is asked to remain alert.*

> ***Law Enforcement Warning (LEW).*** *A warning of a bomb explosion, riot, or other criminal event (e.g., a jailbreak). An authorized law enforcement agency may blockade*

*roads, waterways, or facilities, evacuate or deny access to affected areas, and arrest violators or suspicious persons.*[13]

When using IPAWS for a pre-planned event, the alerting authority has the ability to write alert messages in advance to properly communicate the message. Engaging PIOs to develop message templates, various expected messages, and a communications plan will benefit the event. Appendix J, Model Public Affairs Communications Plan, is an example.

Helpful hints for the use of IPAWS for pre-planned events are provided below.

- Each audience, message, and distribution media should be reviewed.
  - Is the audience smaller than the distribution media will reach?
  - Will the message cause more concern to the public than the event?
- It is not recommended that the authority use WEA messages unless it has the ability to include and edit the free-form 90 character <CMAMText> element into the CAP message.
- The WEA message will also allow the alerting authority to make effective use of the <expires> element to keep alerts active for the time of the event. WEA messages, unlike EAS, will be broadcast to phones as they enter the selected area of the alert until the <expire> time.
- EAS alerts will be distributed to the broadcast audience, which is often larger than the intended audience. For an event that is small and limited to a specific area, EAS may not be the best distribution media. Understanding how your local broadcast stations are configured is important in selecting the proper distribution media.

### 6.3.3. *Exercise*

As discussed above, pre-planned exercises provide an excellent opportunity to use alert and notification systems. A major exercise may affect the public and require an alert on its own. A hostile action exercise may provoke fear or even action by the uninformed public that would put them or the exercise participants in danger. For these types of events, a live message may be appropriate.

Exercises can also benefit from the use of simulated alerts. IPAWS provides alerting authorities with access to a test COG for the use of training and exercises. This test COG can be programmed into many IPAWS authoring tools as a separate distribution environment.

The test COG, when properly implemented, directs the authoring tool to a different IPAWS-OPEN environment. This is the IPAWS-OPEN Test Development Lab (TDL) located at the IPAWS Lab at JITC. This will allow users to create and send messages to a test environment without alerting the public.

---

[13] National Weather Service, Operations and Services; Public Weather Services, NWSPD 10-5, *Non-Weather Related Emergency Products Specification* (Instruction 10-518, July 28, 2010)

When using the test environment, users should ensure the following to prevent errant alerts:

- Ensure authoring tool is pointed to the test lab environment.
- Ensure the authoring tool is not pointed to any other environment.
- Ensure other systems, such as alert bells, lights, and e-mail, are disconnected.
- Disconnect the system if it is connected to a radio transmitter.
- Start the testing by sending a Required Weekly Test (RWT) to ensure it is connected to the correct location.
- Use a two-person team—one person to create the message and one person to verify prior to sending.
- Notify alerting authority, 9-1-1, and response agencies that testing is being conducted.
- Use the IPAWS Message Viewer to monitor the results.

### 6.3.4.  IPAWS Message Viewer

The FEMA IPAWS Program Management Office (PMO) has developed an IPAWS Message Viewer. This service can be used by authorized alerting authorities to practice writing and sending IPAWS messages in a closed testing environment at the IPAWS Lab at JITC. To use the IPAWS Message Viewer, the alerting authority must have the following:

- IPAWS-compatible alerting tool (a list of developers can be found at www.fema.gov/how-sign-ipaws)
- MOA with FEMA for Production or Test access
- A training COG identification (ID) and certificate (note: this is not the Production certificate and usually starts with a "15")

The alerting authority must verify that the authoring tool is connected to the IPAWS Lab at JITC and not connected to the IPAWS Production system.

In a web browser, open the website below and enter your training COG ID where it says "[insert COGID#]":

https://ipaws-open.net/ALERT_SERVICES/postedmessages.php?COGID=*[insert COGID#]*

This will bring up IPAWS Message Viewer main page similar to the following:

**IPAWS Message Viewer**

**COGID 1xxxxx**

| Message Identifier | Sent Date | Event Code | Headline |
| --- | --- | --- | --- |

NO POSTED MESSAGE FOUND

Mission   Terms   Accessibility   About

COGID 15xxxx shows under the IPAWS Message Viewer title above with your training COG ID. Listed under the COGID is a table of public messages posted by the COGID. The table contains "Message Identifier," "Sent Date," "Event Code," and "Headline" and will show all the public messages posted within the last 48 hours. The table is sorted by the "Sent Date" and is displayed in Greenwich Mean Time (GMT).

Under the table, the "Mission," "Terms," "Accessibility," and "About" buttons contain required information governing the information displayed in the IPAWS Message Viewer.

The IPAWS Message Viewer website is normally available 24 hours a day, 7 days a week (24/7) for independent alert testing and verification. It should be noted, however, that after-hours support is not available, and any outages that occur will not be repaired until normal working hours.

As new messages are posted, the IPAWS Message Viewer website retrieves a list of posted public messages from the IPAWS Lab web interface to verify posted alerts for training and demonstration purposes.

When you have the IPAWS Message Viewer website displayed on your screen, you will have to refresh the screen each time to see any new messages. The posted public messages will look similar to the following:

## Message Identifier

To see more details on a message, you can click on the "Message Identifier" link, which will open a new page, "Alert Information View", with details of the message, as shown below:

Note that "Message Identifier," "Sender," "Sent Date," and "Headline" are extracted from <identifier>, <sender>, <sent>, and <headline> elements in the posted message Extensible Markup Language (XML) file.

## WEA Text

This is the Wireless Emergency Alerts (WEA) message that would appear on cell phones. This text is created based on the rules for WEA (i.e., 90-character limit, automatically generated if the WEA text parameters are missing). [See page 99, IPAWS document, reference 2].

## EAS Text

This is the Emergency Alert System (EAS) message that would be transmitted via television and radio. This text is created based on the rules for EAS. [See EAS-CAP Industry Group (ECIG) Implementation Guide, reference 3]. The TV text scroll and/or text-to-speech capabilities and specifics vary depending on the broadcaster's technology and configuration. The actual message relayed to the public may be different than what is reflected here.

The EAS text follows the formatting rules below:

"A CIVIL AUTHORITY HAS ISSUED A [text from Event Code] FOR THE FOLLOWING COUNTIES/AREAS: [text from County Code(s)] AT [h:mm AM/PM formatted time from Sent Time] ON [mmm dd, yyyy formatted date from Sent Time] EFFECTIVE UNTIL [h:mm AM/PM formatted time from Expires Time]. Message from [text of Sender Name]. [text from Description]. [text from Instruction]."

## PUBLIC Text

This field indicates whether or not the Common Alerting Protocol (CAP) message was posted to the IPAWS All-Hazards Information Feed. Please refer to IPAWS Program literature for additional information on this dissemination capability.

## NWEM Text

This is the message that would be transmitted via the National Oceanic and Atmospheric Administration (NOAA) Weather Radio All-Hazards system. This text is created based on the rules for Non-Weather Emergency Messages NEWM). [See NOAA document, reference 4].

The NWEM text follows the formatting rules below:

"THE FOLLOWING MESSAGE IS TRANSMITTED AT THE REQUEST OF THE [text from Sender Name]. [Text from Headline]. [Text from Description]. [Text from Instruction]."

## Exchange COGs:

If the CAP message includes the COG-to-COG messaging function, the recipient COG IDs are listed in this field.

**Warning Area FIPS Codes:**
The Federal Information Processing Standards (FIPS) codes (county codes) that would receive the alert are listed in this field.

**Polygons: Yes/No; Circles: Yes/No:**
If the CAP message includes a polygon and/or circle, then a "Yes" would appear here. If a polygon or circle is present, the "Display Affected Area" button is enabled to display the alert-affected area; otherwise, the "Display Affected Area" button is disabled and grayed out.

**All URIs: Yes/No:**
If the CAP message includes a link to external source (e.g., mp3 audio, jpg image), then a "Yes" would appear here along with a link to the file; otherwise a "No" would appear here.
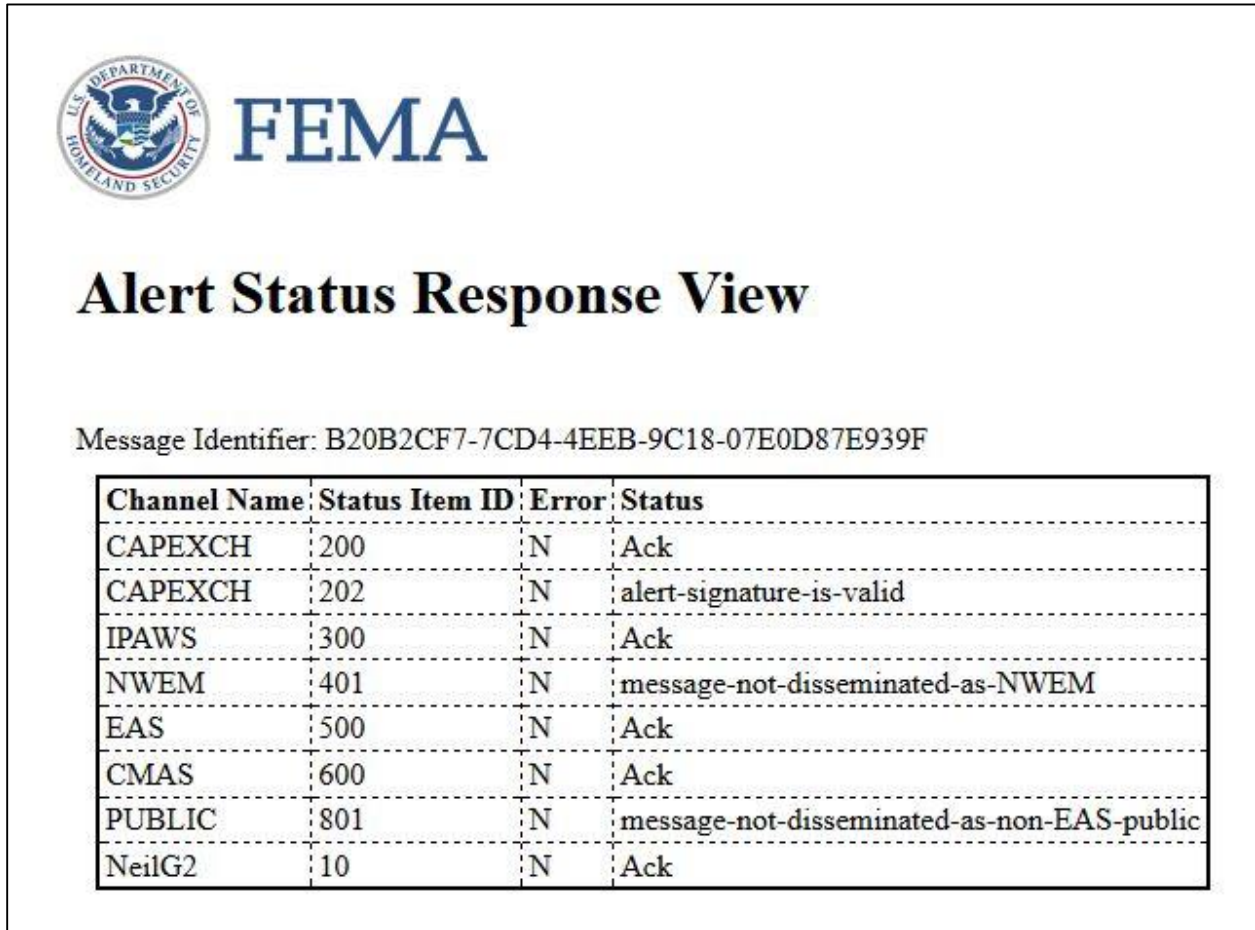
**Display Affected Area:**
If the CAP message includes a polygon and/or circle, then this button will display a map with the alerting area highlighted, for example, in the image below.
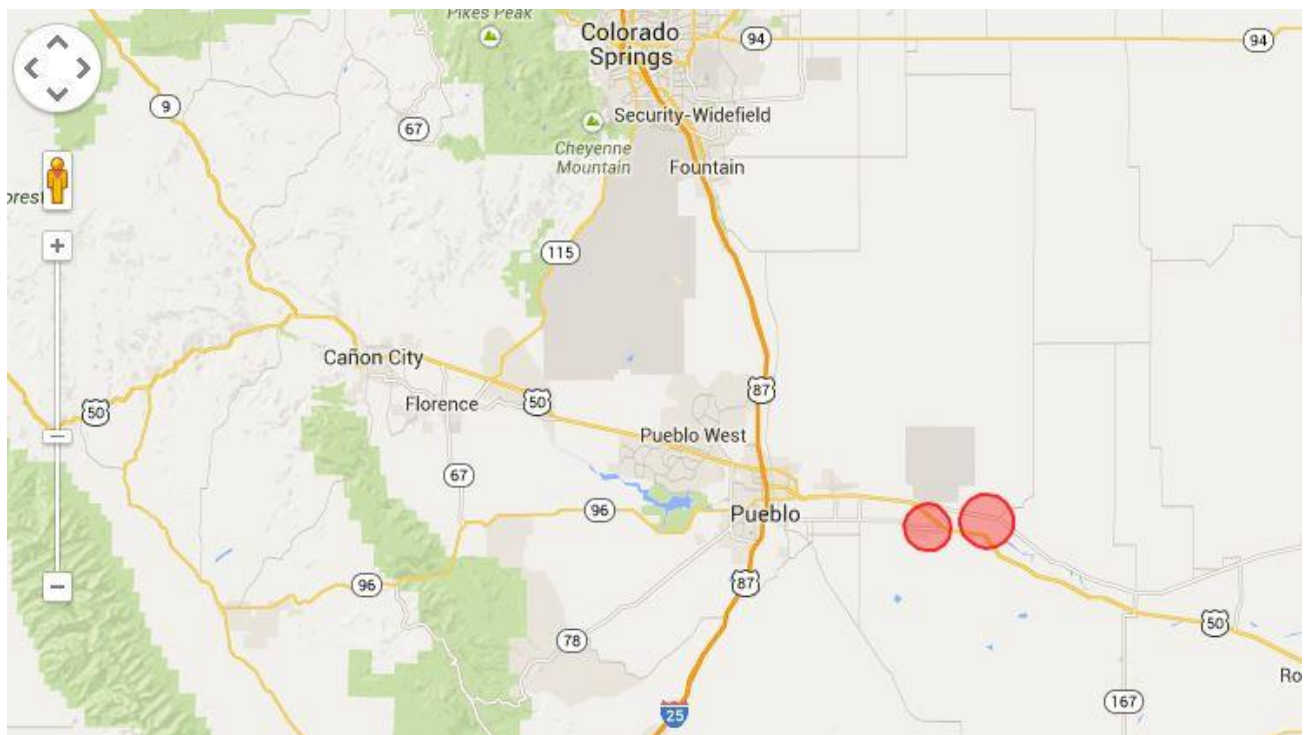
**Display Alert Status:**
This button will open a new page that displays the status codes for this CAP message. A complete table of the codes is located on page 115 of the IPAWS document [reference 2].



The first column, "Channel Name," indicates the device or service from which the status was generated. Any posted alert message with a "300" "Status Item ID" is qualified for IPAWS channel dissemination as a public message for retrieval of posted message list.

| Channel Name | Service | Code range |
|---|---|---|
| WEA Carrier | CMAS Dissemination ACK and Errors | 10+ 100+ |
| CAPEXCH | CAP Exchange ACK and Errors | 200+ |
| IPAWS | Core IPAWS-Profile ACK and Errors | 300+ |
| NWEM | NWEM Specific ACK and Errors | 400+ |
| EAS | EAS Specific ACK and Errors | 500+ |
| CMAS | CMAS Specific ACK and Errors | 600+ |
| Multi-channel | Multi-channel Errors | 700+ |
| Public | Public Non-EAS Specific ACK and Errors | 800+ |

The second column, "Status Item ID," provides the status item code. The fourth column, "Status," provides the text of the status item code. This text describes what the status means. The third column indicates if this status was an error message. Non-error messages usually indicate that the message was processed properly. Together, these codes act as "advice" codes to let you know how IPAWS saw and processed the message that was received.

These codes are the same as those used in the Production IPAWS. Learning the key messages, and where you can see responses in your authoring tool, will improve your ability to send messages and troubleshoot errors in an actual event.

**Display Raw XML:**
This button will bring up the actual CAP message in the XML format. This will assist in understanding how a message is developed and displayed. It is particularly valuable for technical troubleshooting by developers and by IPAWS support staff.



References
1. Common Alerting Protocol, v. 1.2 USA Integrated Public Alert and Warning System Profile Version 1.0 (http://docs.oasis-open.org/emergency/cap/v1.2/ipaws-profile/v1.0/cap-v1.2-ipaws-profile-v1.0.pdf)
2. Integrated Public Alert and Warning System (IPAWS) Open Platform for Emergency Networks (OPEN) IPAWS-OPEN v3.07 Web-Service Interface Design Guidance (document can be requested from ipaws@fema.dhs.gov)
3. Page 30, ECIG Recommendations for an EAS-CAP Implementation Guide, Version 1.0 (http://www.eas-cap.org/ECIG-CAP-to-EAS_Implementation_Guide-V1-0.pdf)

4. National Weather Service Instruction 10-1708
([http://www.nws.noaa.gov/directives/sym/pd01017008curr.pdf](http://www.nws.noaa.gov/directives/sym/pd01017008curr.pdf))

## 6.4.  MESSAGE TEMPLATE DEVELOPMENT

To begin creating message templates, the public alerting plan should be used to identify the types of risks to an agency. With the risks identified, templates with generic messages can be developed to help users send a message more quickly. Care must be used with templates as they will rarely cover all situations, and users must be able to edit the template and remove unrelated information as needed. A public message will have an adverse effect if inappropriate information is in a message and confuses the public.

A CAP message has many components, but the primary fields seen by the public are in the table below. This table was developed to assist the CSEPP Messaging Work Group in developing predefined messages for use with IPAWS. These messages are intended to be formatted to allow acceptance by the four dissemination systems (EAS, CMAS, NWEM, and the all hazards information feed).

For each message, templates should be developed. These templates should contain at a minimum the CAP elements identified below.

| Element Name | Element Used By: | | | Notes and Descriptions |
|---|---|---|---|---|
| | NWEM | EAS | WEA | |
| **eventCode** | X | X | X | Messages intended for EAS, WEA, and HazCollect dissemination must include one and only one instance of this with a value using a same-standard three-letter value. |
| **headline** | X | | | The text headline of the alert message. 160 characters including spaces for NWEM. |
| **description** | X | X | | The text describing the subject event of the alert message. Messages should have meaningful values for the <description>. The content in <description> may be truncated and it is therefore recommended that essential information be addressed first.<br><br>The combination of <description> and <instruction> is <= 160 words for NWEM.<br><description> is 1,800 characters for EAS. |
| **instruction** | X | X | | The text describing the recommended action to be taken by recipients of the alert message. Messages should have meaningful values for the <description>. The content in <description> may be truncated and therefore it is recommended that essential information be addressed first.<br><br>The combination of <description> and <instruction> is <= 160 words for NWEM and 1,800 characters for EAS. |

| Element | Element Used By: | | | Notes |
| Name | NWEM | EAS | WEA | and Descriptions |
|---|---|---|---|---|
| **Parameter CMAMtext** | | | X | This is the WEA message displayed to the public. Message containing free form text limited in length to 90 English characters, but no website or telephone number links. |

### *6.4.1.   Lessons Learned*

The creation of messages and message templates must follow the guidelines of the distribution system used. During CSEPP IPAWS testing, several discoveries were made on how to best use these tools.

<u>General</u>
- **Applications taking the time from the local device, not a network source—**This can result in message failures due to the times of the CAP message being outside the allowable parameters of IPAWS-OPEN. Ensure the device time is correct.
- **Incorrect or not changed default settings—**Several systems allow for the user to set default settings. This includes default end dates, durations, and text from previous messages. If these are not checked and changed as needed for an agency, messages may not have the intended meaning to the public. Use a two-person verification process.
- **Keeping the text from the previous message—**The system can keep the text from the previous message or pre-populate a message. Users must carefully review each element. This can result in duplicate or incorrect messages. Use a two-person verification process.
- **Text cut and paste—**Cutting and pasting text into IPAWS applications resulted in formatting issues in some word-processing programs that may affect the text in the message or prevent the message from being accepted or sent. Using a text editor to remove special formatting and characters works in some cases, but caution should be used, as some web browsers may add formatting to the text that is not visible to the user. Do not cut and paste to create messages.
- **Multiple pages for each message—**Some authoring tools are set to generate a message for only one distribution channel at a time. To send a message to all channels, a message for each channel must be created by the user. This adds time to the alerting process and increases the potential for error among the messages. Develop specifications carefully when selecting a tool. (Refer to Section 4, Selecting Alerting Technologies.)

<u>EAS</u>
The display of an EAS message depends on the equipment at the broadcaster's location. The way a broadcaster sets up its system will have an impact on the way a message is displayed to the public and, in some cases, if it is displayed at all. Two examples of systems to display alerts on televisions are full screen or text crawl. An agency should understand how messages will be displayed before creating messages and templates. (Refer to Section 3.1.4, Commercial Broadcaster Capabilities.)

- Full-screen display is often used by cable broadcasters to display an alert. The message is displayed for a period of time. If the message is long, it is broken down to several pages and displayed. A test sample is shown below.
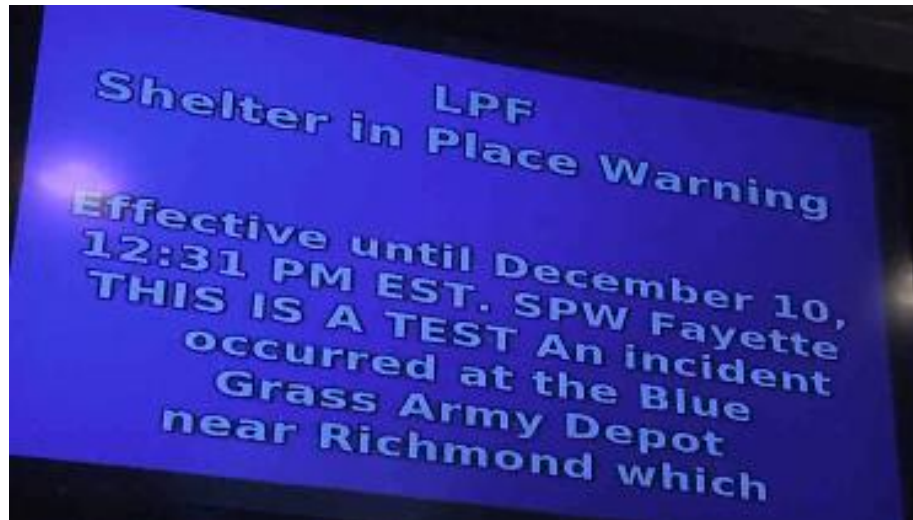
- The text-scroll method involves scrolling text on a regular screen or on a colored banner. In the example below, the text is scrolling over video and is difficult to read.
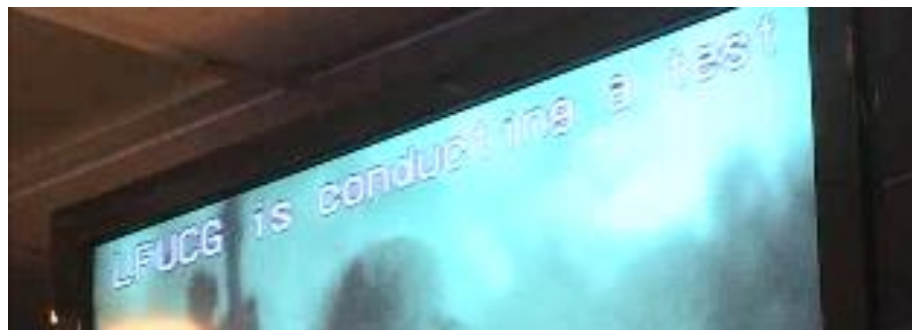


For an EAS message, the system will add a header to the scripted message. The following is an example of an EAS header after the CAP to EAS conversion in the displayed message:

```
ZCZC-CIV-FRW-008101+0129-3501901-LLLLLLLL-
Message from CO Pueblo County Sheriff's Office,Pueblo,CO.
```

This header is displayed by the EAS distribution point as something like this:

> *Civil authorities have issued a Fire Warning for the following Colorado counties: Pueblo. Effective until December 17, 3:31 PM EST.*

After the header, the text from the description and instruction will be added. The time listed in the header comes from the sent time and duration or expire time. This may not be the same as the time listed in the text of the message, which may lead to confusion by the public.

This header is added to the text message and can extend a message to be longer then intended when it is created. When the message becomes too long, the system will simply end the message at the limit defined by the broadcaster. Decoder text crawls can be set to loop a number of times or for message length, which often ends at 2 minutes. This can result in the loss of some of the message. The message shown below ended on the word "to" after 2 minutes the first time it was displayed, and faded out and ended at the end of the word "this" after 2 minutes the second time it was displayed. An agency should understand how messages will be displayed before creating messages and templates. (Refer to Section 3.1.4, Commercial Broadcaster Capabilities.)
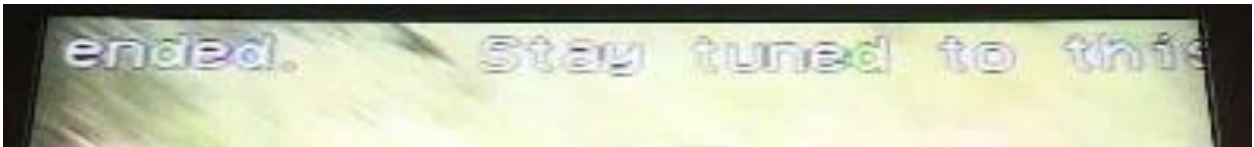


The distribution systems use text-to-speech for the audio from CAP messages unless an audio file is attached to the message. This will have an impact on the way certain words are pronounced. This may affect the message, but testing also found that the use of characters also had an impact on the message.
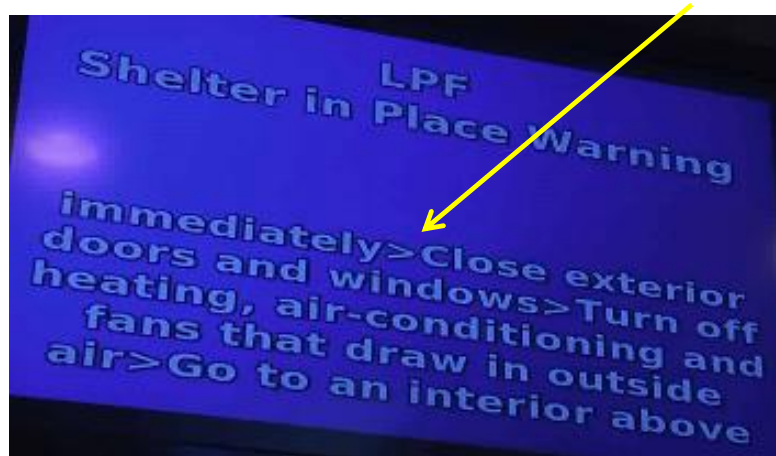


A text-to-speech reader may translated the "-" as "dash" or "to" and ">" as "greater than" in the message audio. This could lead to public confusion. Not all systems translate these characters the same way. An example is the use of the symbol "#" which can be translated as "hashtag" by one system and "pound sign" by another.

Some messages may use carriage returns to go to the next line and break up the message to be more readable. Some origination systems used spaces for the carriage return, but one origination system simply ignored the carriage return. This causes text to run together and affect meaning. The screen shot below shows an example where the fact that the impact includes "Southeast 2" may be lost to the viewer.
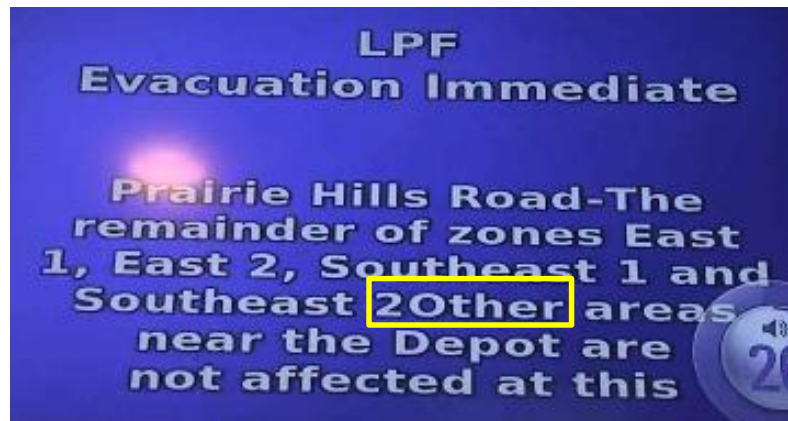
The CAP message also will allow an operator to include a picture, audio, or video. These are called a <resource> element in CAP. If there is one present, it may replace the Description and Instruction in the displayed message to the public, but most currently deployed EAS devices do not support video or pictures, only audio. The Authoring tools each handle these elements differently. Some tools will allow you to record on the fly; others need another device to record the message. Some tools will allow you to upload the file to their system, while others require you to place the message in the agencies publicly available website, then add a link into the CAP message. This is a powerful tool, but requires some planning.

**WEA**
WEA messages are limited in the size of the message. Agencies must plan ahead on the best way to use this distribution channel. Most systems allow users to use the 90-character free-form text element of a CAP message called <CMAMtext>.

If the <CMAMtext> is not present, the wireless provider will use the following CAP elements to create the message:
- "What is Happening"—based on CAP Alert <eventCode> element
- "When the Alert Expires"—based on CAP Alert <expires> element
- "What Action Should be Taken"—based on <eventCode> for two special cases and <responseType> elements for other allowed CMAS event codes
- "Who is Sending the Alert"—based on CAP Alert <senderName> element

WEA messages are displayed on phones differently depending on the software of the phone. The illustration below shows two phones with the same message. On one phone, the <CMAMtext> CAP element was followed by a message that was a combination of the <Urgency> and <Severity> CAP elements.

Alerts display differently on phones
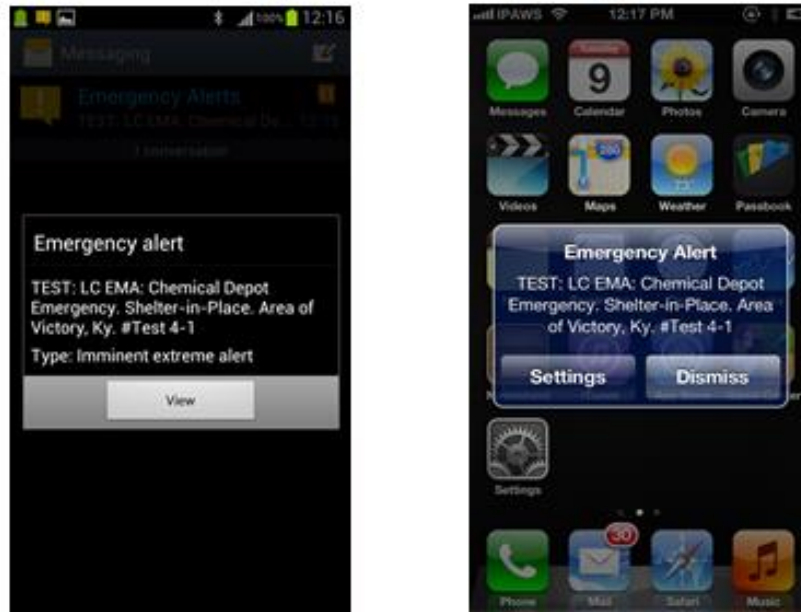
The phones can also store previous messages received.



Multiple Alerts Displayed
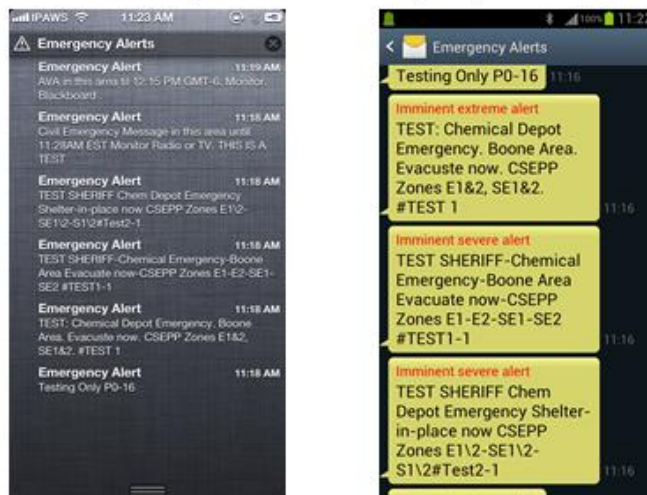
It is important to understand how the text that will be displayed and the importance of the 90-character limit. There is a helpful document on the creation of WEA messages. The U.S. Department of

Homeland Security Science and Technology Directorate contracted research by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland. The study, *Comprehensive Testing of Imminent Threat Public Messages for Mobile Devices*, provides some useful suggestions. The project that created this document was described as follows:

> *This project sought to determine the optimized message contents of imminent threat wireless emergency alert (WEA) messages delivered over mobile communication devices. This report presents findings for the first WEA messages disseminated about imminent threats (i.e., first alert messages) from two research phases with U.S. adults: (1) eight experiments, seven focus groups and 50 think-out-loud interviews; and (2) a survey of an actual "real world" severe flood in Boulder, Colorado. It also integrates findings from across study methods and provides actionable guidance and considerations for optimized message contents of imminent one-hour-to-impact threat alerts delivered over mobile communication devices.*

This document is available at the Homeland Security Digital Library[14] (HSDL), which is sponsored by the U.S. Department of Homeland Security's National Preparedness Directorate, FEMA and the Naval Postgraduate School Center for Homeland Defense and Security.

One of the major recommendations from this study is the order of information in a WEA message, which is as follows: the source of the alert, guidance, hazard, location, and time. WEA message size limits can lead to confusion. The study discussed the issue of a message that was not clear to the receiver and found that messages without clear direction as to the action to take and to whom the message applied may be ignored. The study stated:

> *These findings suggest that the core content of a public alert and warning is: Tell people exactly what to do (guidance), describe why they should do it (hazard) and by when (time). Those who prepare future public alert and warning messages might consider emphasizing these content topics, but not to the exclusion of the others.*[15]

An agency should work with their PIO to develop messages and templates when possible. Having a template set that can be easily adjusted by users is a good solution.

**Polygons**

The CAP message allows users to identify a specific area for the alert. This is done by including a geographic information system (GIS) polygon in the message. Systems may do this differently. Many systems include a map tool to draw an area; other systems will allow users to create a polygon and then import the coordinates into the authoring tool. When using a third-party system, caution should be

---

[14] U.S. Department of Homeland Security. 2014. *Comprehensive testing of imminent threat public messages for mobile devices.* Accessed online September 28, 2015. http://www.hsdl.org/?view&did=763688

[15] U.S. Department of Homeland Security. 2014. *Comprehensive testing of imminent threat public messages for mobile devices.* Page 2. Accessed online September 28, 2015. http://www.hsdl.org/?view&did=763688

exercised that the polygon is in an acceptable CAP format. Two examples of ineffective polygons follow:

- A polygon that consists of three points, two of which are the same. This polygon is a straight line. The message may go through, but may not alert anyone.
- A polygon with multiple points, drawn by hand, similar to an existing CSEPP zone. While the message contains fewer than 200 points and is accepted by IPAWS-OPEN, it contains more than 100 points, so it fails WEA validation and is not sent out.

Wireless providers also use this information differently. Users should understand how wireless providers in their jurisdiction use this information so they can create effective messages. (Refer to Section 3.1.5, Wireless Provider Capabilities, for more information.)

## 6.5. PUBLIC EDUCATION

Public education is important to emergency management; including alert and notification into the existing education program is the best option. An agency's name or acronym should also be integrated into public education programs. This will allow the public to see and recognize the authority before it appears on their phone in an emergency message. Using the same alert log-off name or acronym in routine public messages will accustom the public to them.

An agency should educate the public on IPAWS and WEA before the need to use them arises. Preparing the public will increase the likelihood that the public will take actions to protect themselves. There are two great sources for education ideas. The IPAWS website[16] has links to public service announcements and other resources that can be used. Another good resource is the California Governor's Office of Emergency Services (OES) alerting website.[17] California has developed this website to educate its public on WEA and alerting. This website has good simple information in infographic format on how WEA works. The site also has some frequently asked questions and handouts.

Integrating IPAWS and alerting into pre-planned events is another way to educate the public. Spreading the word prior to and at events provides the public with more exposure to the alerts. Caution should be exercised to not over-use the alerting tools, which may lead the public to complain or even opt out of alerts. Appendix J, Model Public Affairs Communications Plan, can be used to communicate a pre-planned event.

---

[16] Federal Emergency Management Agency. 2015. "Informational materials." Accessed online September 28, 2015. http://www.fema.gov/informational-materials
[17] California Governor's Office of Emergency Services. 2014. "Wireless emergency alerts." Accessed online September 28, 2015. http://www.calalerts.org/

## Appendix A – Implementation Checklists

Implementation checklists and directions for signing up for IPAWS can be found on the following pages and as an attached Word file.

*The remainder of this page intentionally left blank.*

# Planning Checklist

## Current Environment

### Define the Threats

| Threat | Preparation Time | Onset | Geographic Impact Area | Severity | Likelihood |
|--------|------------------|-------|------------------------|----------|------------|
|        |                  |       |                        |          |            |
|        |                  |       |                        |          |            |
|        |                  |       |                        |          |            |
|        |                  |       |                        |          |            |
|        |                  |       |                        |          |            |
|        |                  |       |                        |          |            |

### Define the Populations

| Population | Available Communications Mediums | Language | Notes |
|------------|----------------------------------|----------|-------|
|            |                                  |          |       |
|            |                                  |          |       |
|            |                                  |          |       |
|            |                                  |          |       |
|            |                                  |          |       |
|            |                                  |          |       |

### Available Technologies

| Technology | Target Population | Notes |
|------------|-------------------|-------|
|            |                   |       |
|            |                   |       |
|            |                   |       |
|            |                   |       |
|            |                   |       |
|            |                   |       |
|            |                   |       |

**Goals and Objectives**

| | |
|---|---|
| **Goal 1** | Objective 1.1: |
| | Objective 1.2: |
| | Objective 1.3: |
| **Goal 2** | Objective 2.1: |
| | Objective 2.2: |
| | Objective 2.3: |
| **Goal 3** | Objective 3.1: |
| | Objective 3.2: |
| | Objective 3.3: |

☐   **Research systems**

Research the systems by system type; for example, research sirens, public address, and telephone notification systems, but not the specific vendor.

☐   **Select systems to meet goals and objectives**

Determine what and where systems are needed. An effective solution will include multiple systems. Examples include the following:
- Sirens with public address at two city parks and the downtown walking mall
- Sirens on the edge of the city
- IPAWS for the entire county
- Subscription service for summer residents

☐   **Develop Alert and Warning Plan**

Develop a plan using the information gathered.

☐   **Review Plan with stakeholders**

Review the plan and refine as needed. More input often provides for a better plan.

☐ **Develop Memorandums of Understanding (MOUs) with neighboring jurisdictions**

Contact other jurisdictions to determine if service can be shared or used as a backup system for the selected systems.

# Technology Checklist

☐ **Develop functional specifications for each system**

Define specific functional requirements for the system to meet the needs of the agency.

☐ **Select procurement method for each system**

Determine the procurement method to use (RFP, State contract, direct purchase, etc.).

☐ **Document life-cycle costs**

Conduct a life-cycle cost analysis to determine if the solution can be supported.

☐ **Procure system**

☐ **Install system**

☐ **Perform acceptance testing of system**

☐ **Train all users on the system**

☐ **Notify the public on the abilities of the system**

☐ **Begin operations with systems**

# Integrated Public Alert and Warning System (IPAWS) Collaborative Operating Group (COG) Checklist

☐ **Select IPAWS-compatible software**

Software should be successfully tested in an IPAWS-OPEN test environment. Refer to IPAWS-OPEN Developers (http://www.fema.gov/private-sector-0#psdevelopers) for approved vendors.

☐ **Complete web-based training: IS-247a Integrated Public Alert and Warning System.**

https://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=is-247.a

The course should take approximately 2 hours to complete and is a prerequisite for full access to IPAWS-OPEN for the purpose of public alerting. Upon completion, please send a copy of the course completion certificate to FEMA at ipaws@dhs.gov and the state coordinator.

☐ **Apply for a Memorandum of Agreement with FEMA**

Download the IPAWS Memorandum of Agreement (MOA) from http://www.fema.gov/library/viewRecord.do?id=6019, review the instructions, complete, and scan. Please e-mail the scanned application directly to FEMA at ipaws@dhs.gov. In the subject line of the e-mail, indicate "Operational COG Application." The FEMA MOA Coordinator will prepare and return the MOA for signature after it is submitted.

☐ **Apply for public alerting permissions**

Once your MOA has been initially approved by the FEMA MOA Coordinator and your selected IPAWS-OPEN Developer has indicated they are capable of sending public alerts, the FEMA MOA Coordinator will e-mail you an application for PUBLIC ALERTING PERMISSION and RULES OF BEHAVIOR. Keep blank copies of the Rules of Behavior. You may complete and send to ipaws@dhs.gov and your state coordinator.

Alerting authorities (local jurisdictions) must complete an application defining the types of alerts they intend to issue and the extent of their geographic warning area. The application for IPAWS PUBLIC ALERTING AUTHORITY will be provided when you apply for a COG MOA, along with contact information for a designated state coordinator.

☐ **Train all system users**

Each user should be identified by the agency and granted permission to use the system. Each user should complete the equipment-specific training, IS-247a "Integrated Public Alert and Warning System," and sign a copy of the Rules of Behavior. All records should be maintained by the agency. Some states may request copies.

☐ **Install COG certificate**

You will get several communications from the IPAWS Program Management Office (PMO). These include the COG identification (ID) number, a digital certificate, and passwords. All of these must be protected. The certificate will need to be uploaded to the selected software. This can be done by the agency or the vendor. You may also request or receive a second COG ID for access to the lab environment. This can be useful to train users, but caution must be used to prevent accidental activation or sending a live message to the lab site.

☐ **Apply for National Weather Service (NWS) permissions**

To apply for access, the application must be completed online at https://ocwws.weather.gov/cog/login.php. To complete this application, the authority must have their approved COG ID.

# Operational Checklist

**Develop policies, procedures, and guidelines checklist**

☐ **Identify the team**

    ☐ Assign team

    ☐ Assign tasks

☐ **Research systems and needs**

☐ **Determine documents**

    ☐ Decide documents and types

    ☐ Outline

    ☐ Assign writing tasks

☐ **Draft documents**

☐ **Review draft documents**

☐ **Publish**

☐ **Use**

☐ **Update**

☐ **Publish final document**

☐ **Annual review of all documents**

**Training checklist**

- ☐ **Identify training needs**
  - ☐ Equipment
  - ☐ Procedures
  - ☐ IPAWS requirements
  - ☐ Message creation

- ☐ **Conduct training**
  - ☐ Equipment
  - ☐ Procedures
  - ☐ IPAWS requirements
  - ☐ Message creation

- ☐ **Document training**
  - ☐ Determine what must be documented
  - ☐ Develop documentation files
  - ☐ Document attendance, curriculum, and trainer

- ☐ **Conduct regular refresher training**
  - ☐ Equipment
  - ☐ Procedures
  - ☐ IPAWS requirements
  - ☐ Message creation

**Exercise and regular use checklist**

☐ **Develop regular testing routine**

☐ **Identify regular uses**

    ☐ Begin use on regular events

☐ **Integrate into exercise program**

☐ **Update operations**

    ☐ Procedures

    ☐ Training

    ☐ Routine use plans

# IPAWS Sign Up Directions

The IPAWS PMO provided the following graphic and text from the "Template: Emergency Communication Plans and IPAWS."



1. Select IPAWS compatible software
   - Access to IPAWS is free; however, to send a message using IPAWS, an organization must procure its own IPAWS compatible software.
     i. You should ensure that the software that is chosen meets your organization's specific requirements
   - Consult with your software developer to ensure your system is IPAWS-OPEN compatible and provides the capabilities that your organization requires.
   - For a list of private sector developers who have access to IPAWS-OPEN, please view the list of IPAWS-OPEN developers at http://www.fema.gov/how-sign-ipaws.
2. Apply for a Memorandum of Agreement (MOA) with FEMA
   - To become a COG, a MOA governing system security must be executed between the sponsoring organization and FEMA. Each MOA is specifically tailored to the sponsoring organization and their interoperable software system.
   - Download and complete the IPAWS Operational COG Application: http://www.fema.gov/media-library/assets/documents/27077?id=6019
   - Email this application directly to FEMA at: IPAWS@FEMA.DHS.GOV. Please indicate in the subject line of the email "COG Application."
   - The FEMA COG coordinator will prepare and return the MOA for signature after it is submitted and assign a COG identification (ID). After being signed by the applicant, the MOA will be routed for FEMA signatures. A copy of the executed MOA and the COG-specific digital certificate will be returned to the sponsoring organization. Both the

COG ID and digital certificate are necessary to configure the IPAWS compatible software system. After completing these steps, the organization will have the capability to exchange messages and content between COGs. Please note, these messages will not be sent to the public.

3. Apply for public alerting permissions
   - If applicable, you will receive a public alerting application along with your unsigned MOA. This application must be signed by the designated state official.
   - Complete this application defining the types of alerts a COG intends to issue and the extent of its geographic warning area.
     i. The contact information for the designated state reviewer will be provided with the public alerting application.
   - This form will be submitted for approval to:
     i. The State of {State} at: examplepoc@state.gov
   - Once the signed form is received, please send it to IPAWS@FEMA.DHS.GOV.
4. Complete IPAWS web-based training
   - Complete IS-247.A http://training.fema.gov/EMIWeb/IS/is247a.asp
     i. The goal of this course is to provide authorized public safety officials with:
        1. Increased awareness of the benefits of using IPAWS for effective public warnings
        2. Skills to draft appropriate, effective, and accessible warning messages
        3. Best practices in the effective use of Common Alerting Protocol (CAP) to reach all members of their communities
     ii. The course should take approximately two hours to complete and is a prerequisite for full access to IPAWS-OPEN for the purpose of public alerting. FEMA does not provide training on third-party authoring software. Contact your vendor for any software support questions.
   - Send the Certificate of Achievement to:
     i. The State of {State} at: examplepoc@state.gov
     ii. FEMA at: IPAWS@FEMA.DHS.GOV

**Completing the application**

Once the public alerting application and web-based training are complete, specific alerting permissions will be implemented in IPAWS-OPEN. At that point the individual members specified by the COG will be able to send alerts and warnings in the geographically prescribed areas.

Initial functionality includes the ability to access and send alerts through:
- ✓ the Emergency Alert System (EAS)
- ✓ the National Weather Service (NWS) All-Hazards Emergency Message Collection System for NWS-approved alerting authorities
- ✓ Wireless Emergency Alerts (WEA), depending on local implementation by commercial mobile service providers.

Go to http://www.fema.gov/alerting-authorities for a list of emergency management organizations with access to IPAWS for public alerting.

The {State} Emergency Management and Homeland Security Director recommends going to the FEMA IPAWS website at www.fema.gov/ipaws to view a short five minute video about IPAWS before beginning the process of implementing IPAWS in your jurisdiction.

In addition to the introductory video, IPAWS informational materials, including the "IPAWS Toolkit for Alerting Authorities," can be found at http://www.fema.gov/informational-materials and at statewebsite@state.gov/ipaws.

# Appendix B – Model Alert Planning Tool

The *Model Alert Planning Tool* document can be found as an attached Excel file; directions for the tool can be found on the following pages.

*The remainder of this page intentionally left blank.*

# Alert and Notification Planning Tool

Alerting authorities can use this tool to capture the alerting needs of their jurisdiction and use this information to determine the best alerting and notification systems to use.

Each tab collects information on the needs of the jurisdiction. These can be used to develop a comprehensive alert and notification plan. This tool should be used by the planning group to capture the information. The first two tabs (Audience and Events) can be done in any order; afterwards, each tab should be completed in order. Many of the fields in the spreadsheet are shared between tabs, so use caution when deleting information. Your software may require an action to populate the information between tabs, like a "calculate" button on the lower left screen in MS Excel 2010.

## Audience
List each potential audience in your jurisdiction that may need to receive an alert and notification. These should include residents, visitors, major gatherings, speech and hearing impaired, etc.

For each audience, list a description so that it is clear who the audience is. This may lead to having to add additional audiences. Each audience that requires a specific type of alert method should be listed separately. For example, while school children may be residents, they should not be grouped with elderly residents. This can be used to group based on audience and location such as schools, homes, care facilities, etc.

## Events
List each potential event that may require an alert or notification to the public to protect life or property. Each event should be described.

As each event is described it may result in the addition of other events, or groupings of events to a single event group or type.

## Event_Attributes
The events will populate the Event Attributes tab. For each event, attributes should be identified. The spreadsheet provides pull-down menus for each attribute. The following table lists the attributes. As this is being done, new events may become needed. Return to the Events tab to enter them.

If the User wants to change these, unhide columns "I" through "M" and edit the table.

| Prep Time | Onset | Impact Area | Severity | Likelihood |
|-----------|-------|-------------|----------|------------|
| None | Instant | Blocks | None | 0% to 20% |
| Minutes | 1 to 20 minutes | Cities | Minor | 21% to 40% |
| Hours | 21 to 60 minutes | Part of county | Moderate | 41% to 60% |
| Days | Hours | County | Major | 61% to 80% |
| | Days | Multi-county | Severe | 81% to 100% |

**System_Audience**

List all available alert and notification systems down column A. The audiences will populate across the top row. For each audience, mark the system that may be used to communicate to that audience.

This can be an "X," a "P" for primary and an "S" for secondary, or "1, 2, 3" for the order they can be used.

Next, list any proposed or in-progress systems and mark the audiences.

Lastly, make sure that all audiences have some means of communications.

**Event_Systems**
The systems will populate from the System_Audience Tab, and the events will populate the top row. For each event, mark the system that may be used to effectively communicate to the public for the event listed.

This can be an "X," a "P" for primary and an "S" secondary, or "1, 2, 3" for the order they can be used.

**Advantages**
This tab is optional, but can be helpful in the planning and, more importantly, in exercise planning. For each system, list advantages and disadvantages of the specific system. This will assist in selecting the best solutions for the final plan and procurement.

Then, list how the effectiveness of the system could be measured. This can be used to improve the use of the systems in the future and to develop exercise objectives.

**Notes**
The Notes tab is set up for use as a planning tool in a group setting. The Notes tab allows you to capture questions and information during the use of the tool. The note type is a pull-down menu (unhide Column "F" to edit). The source is who asked or will perform the action. Then the note text describes the issue.

This can also be used when you pass the data around for review to capture questions and comments as needed.

# Appendix C – Model IPAWS Requirements Document

The *Functional Requirements for Model County Alert Origination System* document can be found on the following pages and as an attached Word file.

*The remainder of this page intentionally left blank.*

# Functional Requirements
# for
# Model County
# Alert Origination System

# Table of Contents

# 1. ALERT AUTHORITY SYSTEM SPECIFICATIONS

Model County has determined that the alert and warning of emergencies and dangerous situations to residents and visitors of Model County is a critical function of public safety. To assist the county with ensuring the broadest distribution of alerts and warnings to the public, the Emergency Telephone Notification System (ETNS) and the Integrated Public Alert and Warning System (IPAWS) will be adopted as resources.

The requirements in this document for a web-based alerting system for use by Model County to initiate telephone messages to the public switched network and Common Alerting Protocol (CAP) messages to the IPAWS-Open Platform for Emergency Networks (IPAWS-OPEN) gateway are based on the needs and expected functions of Model County. The system is expected to generate alerts for dissemination to the following:
- Telephones (wireline and voice over Internet Protocol [VoIP])
- Wireless phones (voice and text)
- Emergency Alert System (EAS)
- Wireless Emergency Alerts (WEA)
- National Oceanic and Atmospheric Administration (NOAA) Weather Radio HazCollect system
- E-mail
- Social Media

# 2. DEFINITIONS

**Common Alerting Protocol (CAP)**—CAP is a digital format for exchanging emergency alerts that allows a consistent alert message to be disseminated simultaneously over many different communications systems. CAP is a standard of the Organization for the Advancement of Structured Information Standards (OASIS).

**Collaborative Operating Group (COG)**—A Federal, State, local, tribal, or territorial alerting authority that applies for authorization to use IPAWS and is designated by IPAWS as a Collaborative Operating Group or "COG." A COG may have members from multiple organizations (e.g., a regional mutual aid organization).

**Emergency Notification System (ENS)**—ENS is a set of functions used by an alerting authority to facilitate the one-way dissemination or broadcast of messages to one or many groups of people. ENS is used to notify or alert a group of individuals of a pending or existing emergency situation.

**Integrated Public Alert and Warning System (IPAWS)**—IPAWS is a modernization and integration of the nation's alert and warning infrastructure that will save time when time matters, protecting life and property.

**IPAWS–Open Platform for Emergency Networks (IPAWS-OPEN)**—The Federal alert aggregator that receives and authenticates messages transmitted by alerting authorities and routes them to existing and emerging public-alerting systems.

**System**—For this document, a system is a set of hardware, software, and services used by an alerting authority user to compose, send, and/or receive an alert message to and from IPAWS-OPEN.

## 3. GENERAL SPECIFICATIONS

A. All equipment provided shall comply, where applicable, with industry standards. Examples of these standards are Underwriters Laboratories (UL) approval, American National Standards Institute (ANSI), Open Systems Interconnection (OSI), and Institute of Electrical and Electronics Engineers (IEEE).

B. All systems shall be capable of complying with the Federal Communications Commission (FCC) Communications Security, Reliability and Interoperability Council (CSRIC) IV's Work Group 3 (WG3) EAS Security Subcommittee Report best practices.

C. The system shall be able to operate in ambient temperatures between 35 degrees (°) Fahrenheit (F) and 100° F and relative humidity from 0 percent to 95 percent for a period of at least 48 hours without failure or reduced functionality.

D. The system shall have a method (such as e-mail or text notifications to staff) for reporting the monitoring, logging, and discrepancy capabilities necessary to support troubleshooting and ongoing operations and maintenance.

E. The system shall be able to interface with other device management or monitoring systems using standard protocols such as Simple Network Management Protocol (SNMP) or Common Management Information Protocol (CMIP).

F. There shall be two hard copies (paper) and one soft copy (CD or DVD) of all documentation relating to the system. Documentation shall include the following at a minimum:
   1. Manufacturer technical and maintenance manuals required to support the solution
   2. Operations documentation, which must include backup and recovery procedures and recommended maintenance processes
   3. User's manuals for all systems, sub-systems, and applications
   4. Documentation supporting the operating system (OS)
   5. Final as-built drawings; these drawings can be provided in Visio or another agreed-upon format

G. The system shall be capable of posting the text from the alert to a social media site, including, at a minimum, Facebook and Twitter.

H.   The system shall be able to send both sent and received alerts to an e-mail address or distribution list with the full information and not to a link to another location.

I.   The system shall be able to send alerts to wireless phones via text messaging.

## 4. USER DISPLAY SPECIFICATIONS

A.   The system shall have the ability to adjust colors per user profile log-in to aid users that have difficulties with some colors.

B.   The system shall have the ability to allow user changes or administration to lock the screen configuration. This feature must be controlled by the user's log-on profile (i.e., the screen configuration could be created and modified by all users or could be locked and only configurable by a system administrator).

C.   The system shall use colors that are visible to a visually impaired or colorblind user.

D.   The system shall support features used by visually impaired call takers to magnify or augment parts of the screen.

E.   The system shall be capable of using a standard IBM PC 101–style keyboard.

F.   The system shall be capable of using a standard three-button scrolling mouse.

G.   The system shall require the user to navigate the least number of screens not more than three screens to create and send an alert.

H.   The system shall provide visual alerts for specific CAP elements and values configured in the system by the user.

I.   The system shall provide the ability to connect external visual and audible alert devices such as strobes, buzzers, and e-mail or text message.

J.   If the system operates on another hardware system such as a personal computer (PC), the system shall include an OS. The OS supporting the PC shall be fully supported by the system for a minimum of a 5-year time period after acceptance.

K.   The central processing unit (CPU) must be configured with robust and reliable processors along with all necessary data and audio interfaces. The CPU must also be configured with properly sized power supplies, memory, and hard drives to support 100 percent of all software installed on the system without reducing user functions.

L.   The system shall include malware and antivirus protection for all servers and workstations in the system. The system shall support periodic scheduled malware and antivirus updates.

M.   The system shall support the ability to print screens, files, forms, and logs to an external printer.

N.   The system shall support a master timing source from an agency (local time source) or external (Internet or radio) source. The master timing source shall support, at a minimum, Ethernet Network Timing Protocol (NTP) and other sources defined in National Emergency Number Association (NENA) 04-002, *PSAP Master Clock Standard*.

O.   The system shall display a message preview to the user of the entered data in the format it will most likely be displayed to the public prior to sending the alert for each distribution channel selected.

P.   Message elements shall be presented to the user in a pull-down list where the defined values are known.

Q.   Pull-down lists shall be limited by allowable elements of the distribution channel selected.

R.   Alert distribution channels available to the user shall be configurable by the system administrator for each user or user groups.

S.   The system shall allow all configuration settings and changes from the keyboard.

## 5. USER INTERFACE SPECIFICATIONS

A.   The system shall require unique user log-ons. Each user accessing the solution or workstation shall be required to log on with a user name and password.

B.   Passwords shall be at least six characters long and allow the use of letters (lowercase and capital), numbers, and special characters. Users shall be able to define or create their own unique passwords.

C.   The system shall support at least 100 unique user names for log on.

D.   The system shall allow an administrator to set levels of permissions to access components of the system, such as limiting access to a specific COG or changing templates to specific personnel.

E.   The system shall allow an administrator to set at least five permission levels to access components of the system, such as limiting access to a specific COG or changing templates to specific personnel. These levels will include:

1. Administrator—full access
2. Power User—access to all distribution methods
3. General User—access to distribution but not IPAWS
4. Agency Users—limited access to distribution with the ability to limit access to groups or parts of the database
   a. This level shall be able to be used for multiple separate agencies
5. Limited User—access to create, edit, and use predefined call out lists of agency resources

F. The system shall configure the workstation with the user-defined personalized features that the user has created in his or her profile and log-on permissions.

G. The system shall allow the administrator or authorized user to pre-program at least 200 template messages. It is desirable that the messages be grouped into different situation types to aid in quicker response.

H. The system shall allow the administrator or authorized user to pre-program at least 50 pre-defined CAP v1.2 <area> elements for specific locations/polygons. It is desirable that the areas be grouped to aid in quicker response.

I. All pre-programmed elements shall be available for all COGs configured in the system without requiring copying.

J. The system shall allow the user to select from multiple messages and multiple location templates for a single alert, such as click something for shelter in place for one area, click something else for evacuation in another area, and click something else for standby. Having a template with a checklist where boxes could be checked and where text-to-speech would recognize what boxes were checked would be ideal.

K. The system shall meet uptime of 99.995 percent or better.

L. The system shall be able to generate messages using sub-county Federal Information Processing Standard (FIPS) codes.

M. The system shall be able to generate message locations using an internal or external mapping function to create polygons.

N. Selected polygons shall be checked to ensure that at least one tower is included in the activation area.

O. The system shall support a minimum of two separate COGs to be configured in the system.

P. Each screen shall clearly identify the COG from which the alert will be sent to prevent errors.

Q.  The system shall permit the user to switch between COGs without requiring the restart of the system or logging off.

R.  The system shall be able to allow the administrator to configure the system to default to the test COG.

S.  The system should support configuration of up to 10 separate COGs for backup purposes.

T.  The system shall automatically perform validations of messages to meet CAP, IPAWS, and dissemination system requirements and provide a visible alert and the reason and/or recommended corrections when the requirements are not met.

U.  The system shall pull time and dates from the system time automatically.

V.  The system shall allow the user to change the date and time after pre-populating from the system.

W.  The system shall allow the administrator to set the default duration.

X.  The system shall automatically calculate the time intervals to meet the required formats.

Y.  The system shall support user access from at least two remote sites in addition to the installed location.

Z.  The system shall support at least 20 simultaneous users.

AA. The system shall provide automatic log-off of users for inactivity configurable from 1 minute to 12 hours.

BB. The system shall continue to operate, receive, and forward, if configured, alerts while no user is logged on.

CC. The system hardware shall be located in a secure facility with restricted and monitored access.

DD. The system shall be a set of hardware and software that can be located within the respective agency's facility.

EE. The system shall be able to be connected to a local area network (LAN).

FF. The system shall provide at least two methods of access (e.g., Internet, phone, or e-mail).

GG. The system shall provide text-to-speech abilities for messages, with custom dictionary capability for proper pronunciation of local words.

HH. The system shall provide an audio preview of the message from the message creation page.

II. The system shall be able to record audio messages from the message creation page.

JJ. The system shall automatically fill in elements from the COG information.

KK. The system shall display a message that contains errors and possible solutions for improper alerts when a user attempts to send the alert but provide the capability for the user to override errors and send the alert.

LL. The system shall be able to be configured with the method for which each carrier implements WEA in the COG area to allow the user to select the appropriate area in which to send an alert.

MM. The system shall display, by carrier, the towers that should be activated in the selected area.

NN. The system shall display if a selected area does not include all carriers in the area.

OO. The system shall display a message before sending an alert asking the user if they are sure they want to send the message.

PP. The user shall be able to review all status messages returned from IPAWS-OPEN.

QQ. The user shall have one-click access to a message log to review all actions of the system and IPAWS-OPEN.

## 6. IPAWS INTERFACE SPECIFICATIONS

A. The system shall be able to generate a message in CAP v1.2 and meet the CAP v1.2 USA IPAWS profile v1.0.

B. The system shall be able to send a CAP- and IPAWS-compliant message to both the production and Joint Interoperability Test Command (JITC) test IPAWS-OPEN.

C. The system has been tested and the vendor can provide proof that the system is able to send messages through IPAWS-OPEN to the EAS gateway.

D. The system has been tested and the vendor can provide proof that the system is able to send messages through IPAWS-OPEN to the WEA gateway.

E. The system has been tested and the vendor can provide proof that the system is able to send messages through IPAWS-OPEN to the Non-Weather Emergency Message (NWEM) gateway.
   1. This requires that the vendor has tested with NOAA and the proposed solution is approved and currently delivering calls to the NOAA weather radio NWEM system via IPAWS-OPEN.

F. The system shall be able to send messages through IPAWS-OPEN to the IPAWS All-Hazards Information Feed gateway.

G. The system shall be able to send COG to COG messages through IPAWS-OPEN.

H. The system shall have a simple (i.e., no more than three clicks) means to retrieve the sent message and be able to send an IPAWS cancel or modify message to IPAWS-OPEN.

I. The system shall be able to monitor alerts from other COGs via the Internet feed.

J. The system shall be able to relay alerts from other COGs.

K. The system shall be capable of monitoring at least two other alert systems, such as the National Weather Service (NWS) weather radio, LP1 stations, and satellite stations.

L. The system shall be able to send alerts to a local radio transmitter.

M. The system shall be able to relay alerts from other sources to a local radio transmitter.

N. The system shall be capable of delivering CAP message formats from received and generated alerts to third-party systems such as message boards and other computer systems.

O. The system shall be capable of attaching files such as audio, video, or pictures to the message in a manner available to the various distribution channels.

## 7. MAPPING INTERFACE SPECIFICATIONS

A. The system shall be able to display a map of the COG and surrounding areas to the user.

B. Mapping functionality shall include freehand, polygons, radius, and intersection and shall list features in that polygon after drawn. Features that shall be viewable include telephone devices (primarily landline but also cell/VoIP that have opted in), cell phone towers, and special needs residents and/or facilities (data to be collected by the county).

C. The mapping function shall provide a dynamic display and rendering of different layers based on zoom level.

D.   The system shall accommodate the use of accepted aliases for street names.

E.   The mapping function shall allow a user to select an area on the map to which an alert will be sent.

F.   The mapping function shall automatically take the selected area and generate a CAP <area> element to include in the alert message.

G.   The system shall automatically validate the CAP <area> based on the distribution channel, particularly WEA.

H.   The system shall import Environmental Systems Research Institute (Esri) map files.

I.   The map import function shall be able to be performed by the agency user and not require conversion to other formats.

J.   The system shall automatically take Esri map files and generate a CAP <area> element template that can be included in the alert message.

K.   The system should support imagery using the multi-resolution seamless image database (MrSID) encoding algorithm.

L.   The system shall automatically determine if a selected area extends beyond the COG boundaries and notify the user prior to sending the alert.

M.   The system should be able to input a polygon in a shape (.SHP) and Keyhole Markup Language (.KML) files from another source (such as WebPuff™) to generate a CAP <area> element.

N.   The system shall be able to look up required NWEM geocode values using the "getNWEMAuxData" method on the IPAWS-OPEN interface.

O.   The system shall be able to look up an IPAWS-configured Event Code and geocode permissions by distribution channel using the "getCogProfile" method on the IPAWS-OPEN Interface.

P.   Telephone number databases shall be linked to the map and geocoded to the map database.

## 8. LOGGING AND REPORTING SPECIFICATIONS

A. The system shall have comprehensive logging and reporting capabilities to detail the activity on the system. Actions that shall be logged include, at a minimum, the following:
1. User log-on and log-off
2. User activity (adds, deletes, or changes to data) while logged on
3. All alerts sent
4. All alert and system messages received
5. Alerts from other COGs
6. Visible data to the user (polygons, alerts, etc.)

B. The logging file and process shall be performed in a manner that creates a legal record of the activities and is not editable by users. All records shall have the "write once read many" (WORM) attribute.

C. The system shall provide real-time progress reports of all alerts.

D. The log shall be exportable in part or in whole to an electronic readable and editable format for reporting purposes.

E. The system shall be able to log and store at least 6 months of activities. For a CSEPP event, this can include numerous alerts for different areas and repeated at 8- to 15-minute intervals for the duration of the event, which may last for hours.

F. The system shall be able to query the data to create, save, and print reports in an ad hoc fashion.

G. The system shall be able to generate scheduled reports automatically.

H. The system shall be able to print reports to electronic files and printers.

I. The system should be able to e-mail reports.

J. ENS reports shall also include the following:
1. Time started, duration, and time ended
2. Number of call attempts
3. Results of each call (e.g., busy, no answer, answering machine)
4. Numbers called list
5. Number of successful calls
6. Agency and user that generated calls

## 9. ENS SPECIFICATIONS

A.   The system shall allow the user the ability to listen to the emergency notification message prior to a notification being deployed without having to send an alert.

B.   The system shall comply with all Americans with Disabilities Act (ADA) requirements. This shall include the ability to reach Telecommunications Devices for the Deaf (TDDs) (both Baudot and ASCII) during a field-event launch.

C.   The system shall have the ability to send the notification message to users in a text format as well as voice.

D.   The text-to-speech program shall allow for the use of custom dictionaries for local pronunciation.

E.   The system shall permit an audio message to be created via telephone or a computer and used instead of text-to-speech.

F.   The system shall have a comprehensive interactive notification system for internal call lists and internal departmental communication.

G.   It is preferable that the system have the ability to deliver messages in multiple languages, at a minimum English and Spanish, based on the preference of the registered receiver.

H.   The system shall match at least 99.99 percent of related 9-1-1 records based upon any geographic selection.

I.   The system shall redial or resend alerts to numbers that may not answer on the original call. The system shall redial a minimum of up to three times and be configurable by the user or administrator.

J.   The system shall allow the user to start a new set of calls to only those not reached in the previous message.

K.   The system should have a method to start the recording shortly after the recipient picks up and not have a delay to wait for answering machines. The message may restart on an answering machine beep.

L.   The system shall allow the administrator to tag information as persistent and not overwrite this data on updates.

M.   The system shall allow the administrator to develop static call lists such as call outs for additional personnel or special services, such as a Specialized Weapons and Tactics (SWAT) team.

N.   The system shall be able to generate call lists from additional data elements in the record such as business address, volunteer organization, etc.

O.   The system shall have the ability to adjust the number of calls per minute transmitted to specific areas, services, or providers so as to not overload the delivery systems.

P.   The system shall support all telephone types, including plain old telephone system (POTS), wireless, and VoIP subscribers.

Q.   The system shall use a local call back number and display that number as the caller identification (ID) on alerts. The systems shall use multiple local call-back numbers and display that number as the caller ID on alerts.

R.   The system shall provide a call-back feature where a recipient can call to get the current alert.

S.   The system shall provide a feature to allow the recipient to select a number and be transferred to a recording with additional information.

T.   The system shall allow the sender or other authorized user to stop, pause, or cancel an alert in progress of notification.

U.   The system shall provide the voting or polling ability (such as pressing 1 for no or 2 for yes) for the recipients of calls.

## 10. ENS DATA SPECIFICATIONS

A.   Data stored in the vendor's database for the use of an agency shall be considered the property of the agency and not be shared with other entities without written approval.

B.   The data stored in the vendor's database for the use of an agency shall be available to the agency on request in an agreed-upon electronic format.

C.   The system shall use the telephone numbers provided in the 9-1-1 database.

D.   The selected vendor shall coordinate telephone record uploads and periodic updates, at least quarterly, with the Incumbent Local Exchange Carrier (ILEC); more frequent updates are preferred.
   1.   Final frequency of updates will be negotiated with the selected vendor based on cost.

E.  The system shall have the ability to upload contact data in a bulk format from common files (e.g., CSV, spreadsheet)

F.  The system shall have an "opt in" program that would allow residents to opt in their cell, VoIP, or other phone.

G.  The system shall be able to have the resident associate his or her phone number with multiple geographic addresses (home, work, school, etc.) that shall be validated as a valid address through the system.

H.  The database for "opt in" numbers outside of the 9-1-1 automatic number identification (ANI) database shall be maintained by the selected vendor and shall be updated to the system at least once a day.

I.  The system shall have the ability for the administrator to add additional fields or data elements to the database.

J.  The selected vendor shall provide data security and confidentiality for all data provided by the county, individuals, and other providers. The vendor shall not use this data for other purposes, and a privacy policy shall be provided to the agency and persons "opting in."

K.  The system shall allow users with permissions to perform searches on the data in the database for all fields, but at a minimum:
    1.  Phone Number
    2.  Name
    3.  Address

## 11. TRAINING SPECIFICATIONS

A.  The selected vendor shall provide at least two on-site user training sessions for xx students on the operation of the system. Each trainee shall be provided with a hard copy of training materials.

B.  The selected vendor shall provide at least one system administrator training session for up to five students on system management. Each trainee shall be provided with an electronic copy of training materials.

C.  The selected vendor shall provide at least one face-to-face train-the-trainer user-training session for up to six students. Each trainee shall be provided with an electronic copy of any training materials.

D.   All training shall include a component of sending alerts to the IPAWS Lab at the JITC to view the video feed of alerts received from the deployed system. The selected vendor is responsible for coordinating this with the JITC.

E.   The selected vendor shall deliver two hard copies and two soft copies (CD or DVD) of all training materials to the agency for reference.

F.   All electronic materials shall be in an unlocked format, which will allow for cutting, pasting, printing, and other use as needed by Model County and other users of this system.

G.   The selected vendor shall provide 24/7/365 phone customer support for users to request assistance in using the system. This can include walking a user through the process of creating an alert or answering non-emergency questions.

H.   Web, computer, and/or video training should be available to users as a regular refresher on the processes and procedures of using the system.

I.   The vendor should have available regular refresher training on the systems and new features and functions. This should be available at least annually. Frequency and delivery methods will be negotiated, but vendors shall describe the methods and cost options.

J.   A training interface of the system is required. Users must be able to perform all functions without sending a live alert. The training interface must closely mimic the "live" version but be easily identified as a "training only" interface.

## 12. WARRANTY AND MAINTENANCE SPECIFICATIONS

A.   The selected vendor shall provide updates and upgrades that are released for the system for a period of at least 2 years after installation at no additional charge.

B.   The selected vendor shall support the full functions of the purchased system on an annual renewal basis for at least 5 years without requiring the agency to purchase upgrades or change contract terms. For example, if a feature is included in the service but then later is moved to a separate module by the vendor, Model County expects that the function will still be available to use.

C.   The system shall include a 2-year replacement warranty for all hardware, software, and ancillary equipment commencing upon the final acceptance of the system. The warranty shall provide for resolution of all faults or malfunctions at no additional cost (including shipping) to the agency. The agency reserves the right to begin the warranty period earlier if only minor punch-list items remain unresolved and will provide notice, in writing, to the vendor if this is agreeable.

D. The vendor shall provide 24/7/365 phone support for priority one and two faults. Faults are identified as follows:
1. **Priority One Fault**—A priority one fault is a major system fault that renders the system completely inoperable. These faults shall be resolved within 4 hours.
2. **Priority Two Fault**—A priority two fault consists of major and minor faults that significantly reduce the solution performance and ability to function. These faults shall be resolved within 24 hours.
3. **Priority Three Fault**—A priority three fault is a minor system fault that marginally affects system performance and functionality. These minor faults are operational in nature. These faults shall be resolved within 5 work days.
4. **Priority Four Fault**—A priority four fault is a combination of minor system faults or system user questions. These are faults that have minimal or no effect on system performance and functionality. These faults shall be resolved within 10 business days.

E. The selected vendor shall provide procedures for initiating, tracking, and resolving trouble reports within the limits for each priority level.

F. The selected vendor shall provide an escalation plan to the agency. This plan shall include documentation of the escalation process along with names, titles, and contact information and include the after-hours escalation process if different from normal work hours.

G. The selected vendor shall provide data backups of all databases, configurations, and settings.

## 13. IPAWS SYSTEM SUMMARY WORKSHEET

In the "response" column, Respondents shall indicate with one of the allowable responses (described below) if their solution will provide this function. Each previous requirement, detailed in the specification sections, is listed in the worksheet on the following page. Respondents should review the detailed requirements listed above prior to completing the worksheet.

The three allowable responses are:
- Comply—This indicates that the solution fully provides for the functions listed in the requirement section of this document.
- Partial Comply—This indicates that the solution does part of the function or may accomplish the same function in another manner.
- Not Comply—This indicates that the solution is not capable of performing the required function.

All Partial Comply or Not Comply responses require an explanation of the response in the notes section.

**3 – General Specifications**

| Requirement | Response | Notes |
|---|---|---|
| A. Meets industry standards | | |
| B. Complies with CSRIC EAS Security best practices | | |
| C. Can operate in extreme conditions | | |
| D. E-mail or text for reporting trouble | | |
| E. Interface with other device management or monitoring systems | | |
| F. Provide documentation | | |
| G. Posting to social media | | |
| H. Posting to e-mail | | |
| I. Posting to text message | | |

**4 – User Display Specifications**

| Requirement | Response | Notes |
|---|---|---|
| A. Able to adjust screen colors | | |
| B. Ability to lock screen configuration | | |
| C. Colors visible to visually-impaired or color-blind users | | |
| D. Support features for vision impaired users | | |
| E. Uses standard keyboard | | |
| F. Uses standard 3-button mouse | | |
| G. Navigate no more than 3 screens | | |
| H. Visual alerts for CAP elements | | |
| I. Can connect external devices | | |
| J. PC OS supported for 5 years | | |
| K. CPU supports 100% of all software installed | | |
| L. PC has malware/anti-virus and is updated | | |
| M. Supports printing | | |
| N. Supports master timing source | | |
| O. Previews message to user | | |
| P. Message elements presented in pull-down list | | |
| Q. Pull-down lists limited by allowable elements | | |
| R. Alert distribution channels configured per user | | |
| S. All configuration can be done by keyboard | | |

**5 – User Interface Specifications**

| Requirement | Response | Notes |
|---|---|---|
| A. Require user log on | | |
| B. Password at least 6 characters | | |
| C. Supports at least 100 user names | | |
| D. Administrator can define user permissions | | |
| E. At least five permission levels | | |
| F. Workstation configurable with user-defined features | | |
| G. At least 200 templates | | |
| H. At least 50 pre-planned polygons | | |
| I. All templates available in all COGs | | |
| J. Select multiple messages and areas | | |
| K. 99.995% up time | | |
| L. Use sub-FIPS codes | | |
| M. Generate area from internal or external mapping function | | |
| N. Check polygons for wireless provider towers | | |
| O. Support at least 2 COGs | | |
| P. Clearly identify COG on page | | |
| Q. Switch between COGs without restart | | |
| R. Configure to default to test COG | | |
| S. Support up to 10 COGs | | |
| T. Automatically validate CAP elements | | |
| U. Automatically pull time and date | | |
| V. Allows user to change date | | |
| W. Ability to set default duration | | |
| X. Automatically calculate time intervals | | |
| Y. Support user access from at least two remote sites | | |
| Z. Supports at least 20 simultaneous users | | |
| AA. Automatically log off user for inactivity | | |
| BB. Continue to operate when logged off | | |
| CC. Located in secure facility | | |
| DD. Set of hardware and software located within agency's facility | | |
| EE. Connect to LAN | | |
| FF. At least two methods of access | | |
| GG. Provide text-to-speech with custom dictionary | | |
| HH. Provides audio preview to user | | |

| Requirement | Response | Notes |
|---|---|---|
| II. Able to record audio from message page | | |
| JJ. Complete CAP elements from COG data | | |
| KK. Display errors and solutions for CAP elements | | |
| LL. Configure based on WEA deployment method | | |
| MM. Display carrier and towers that are in alert area | | |
| NN. Display if a carrier is not included in alert | | |
| OO. Display message to verify the user wants to send | | |
| PP. Able to display to user IPAWS-OPEN status messages | | |
| QQ. One-click access to message log | | |

## 6 – IPAWS Interface Specifications

| Requirement | Response | Notes |
|---|---|---|
| A. Able to generate CAP v1.2 messages | | |
| B. Send CAP- and IPAWS-compliant messages to production and JITC test IPAWS-OPEN | | |
| C. Tested, with proof of messages through IPAWS-OPEN to EAS gateway | | |
| D. Tested, with proof of messages through IPAWS-OPEN WEA gateway | | |
| E. Tested, with proof of messages through IPAWS-OPEN to NWEM gateway | | |
| F. Send messages through IPAWS-OPEN to IPAWS All-Hazards Feed gateway | | |
| G. Send COG to COG messages | | |
| H. Retrieve sent message and send cancel or modify messages to IPAWS-OPEN | | |
| I. Monitor alerts from other COGs | | |
| J. Relay alerts from other COGs | | |
| K. Monitor at least two other alert systems | | |
| L. Send alerts to local radio transmitter | | |
| M. Relay alerts from other sources to local radio transmitter | | |
| N. Delivering CAP message formats to third-party systems | | |

| Requirement | Response | Notes |
|---|---|---|
| O.  Ability to attach files to message | | |

**7 – Mapping Interface Specifications**

| Requirement | Response | Notes |
|---|---|---|
| A.  Able to display map | | |
| B.  Mapping functions include freehand, radius, etc. | | |
| C.  Dynamic display of layers | | |
| D.  Supports alias street names | | |
| E.  Supports user selection on the map | | |
| F.  Mapping generates CAP <area> element | | |
| G.  Automatically validate CAP <area> | | |
| H.  Supports import of Esri files | | |
| I.  Map data import can be performed by user | | |
| J.  Support creation of CAP <area> elements from Esri files | | |
| K.  Supports MrSID | | |
| L.  System identifies if area selected is outside of COG boundaries | | |
| M.  Supports import of .SHP and .KML files | | |
| N.  Performs "getNWEMAuxData" | | |
| O.  Look up an IPAWS configured Event Code and geocode permissions using "getCogProfile" | | |
| P.  Telephone number database is geocoded to map | | |

**8 – Logging and Reporting Specifications**

| Requirement | Response | Notes |
|---|---|---|
| A.  System logs activities | | |
| B.  Log is legal record | | |
| C.  Real-time progress reporting | | |
| D.  Log is exportable | | |
| E.  Log holds at least 6 months data | | |
| F.  Able to query data and run ad hoc reports | | |
| G.  Generate scheduled reports | | |
| H.  Print reports to printer and electronic file | | |
| I.  Able to e-mail reports | | |
| J.  ENS reports include call data | | |

**9 – ENS Specifications**

| Requirement | Response | Notes |
|---|---|---|
| A. Permits user to listen to message before sending | | |
| B. Compliant with ADA | | |
| C. Supports text as well as voice | | |
| D. Text-to-speech with custom dictionaries | | |
| E. Audio message created via telephone or computer | | |
| F. Supports call lists | | |
| G. Supports multiple languages | | |
| H. Matches 9-1-1 data to map | | |
| I. Supports redial | | |
| J. Supports new call to those not reached | | |
| K. No time delay for message starts | | |
| L. Supports persistent data | | |
| M. System administrator can create call out lists | | |
| N. Supports creation of additional data fields | | |
| O. Adjust calling speed | | |
| P. Supports all phone systems | | |
| Q. Provides local call back number | | |
| R. Supports call backs from public | | |
| S. Supports transfer for more information | | |
| T. Permits stop, pause, or cancel | | |
| U. Supports voting or polling | | |

**10 – ENS Data Specifications**

| Requirement | Response | Notes |
|---|---|---|
| A. Data is property of agency | | |
| B. Data is available upon agency request | | |
| C. Uses telephone numbers in 9-1-1 database | | |
| D. Quarterly updates with ILECs | | |
| E. Uploads data in bulk format | | |
| F. "Opt in" program for residents | | |
| G. "Opt in" program associates with multiple geographic addresses | | |
| H. Resident-provided "opt in" numbers maintained by vendor | | |
| I. Allows addition of fields | | |

| Requirement | Response | Notes |
|---|---|---|
| J. Provides data security and confidentiality | | |
| K. Provides ability for searches | | |

**11 – Training Specifications**

| Requirement | Response | Notes |
|---|---|---|
| A. Provide user training | | |
| B. Provide system administrator training | | |
| C. Provide train-the-trainer training | | |
| D. JITC test lab component | | |
| E. Provide training materials | | |
| F. Training materials unlocked | | |
| G. Provide 24/7/365 phone support | | |
| H. Web, computer, video refresher training | | |
| I. Refresher training on systems and new features/functions | | |
| J. Training interface | | |

**12 – Warranty and Maintenance Specifications**

| Requirement | Response | Notes |
|---|---|---|
| A. Provide updates and upgrades | | |
| B. Support functions for 5 years | | |
| C. 2-year replacement warranty | | |
| D. Provide 24/7/365 maintenance support | | |
| E. Provide trouble reporting process | | |
| F. Provide escalation plan | | |
| G. Provide back up of all data | | |

# Appendix D – Model EAS Survey Form

The EAS Survey Form can be found on the following pages and as an attached Word file.

*The remainder of this page intentionally left blank.*

# IPAWS EAS Survey

**Station**

| Information Requested | Provide Information |
|---|---|
| Name | |
| Address | |
| Business Phone | |
| 24x7 Phone | |
| FCC License and Frequency | |
| Counties in Broadcast Area | |

**IPAWS Point of Contact**

| Information | Provide Information |
|---|---|
| Name | |
| Title | |
| Address | |
| Business Phone | |
| E-mail | |

| **Is your station staffed 24x7?** | |
|---|---|

**IPAWS/EAS Decoder**

| Question | Answer |
|---|---|
| Type of decoder used | |
| Is the encoder text-capable? | |
| Is the encoder audio-capable? | |
| Is the encoder video-capable? | |
| How often do you poll IPAWS-OPEN? | |

**Do you monitor and rebroadcast the following: (Please list the station.)**

| System | Yes/No? |
|---|---|
| EAS from PEP? | |
| EAS from SR1? | |
| EAS from SR2? | |
| EAS from an LP1? | |
| EAS from an LP2? | |
| EAS from another source? (List sources.) | |
| IPAWS feed from the Internet? | |
| National Weather Radio (NWR)? | |
| Other feeds? | |

| Are any sources set as primary? If so, please list the order. | |
| --- | --- |

| What happens to the message from multiple sources? (For example, a tornado warning from NWR and an SR1 or LP1 Station.) | |
| --- | --- |

**How is your encoder configured for the following event codes? (List the counties it filters for, and the action to re-transmit if automatic or manual. If manual, what action must take place to activate?) Add additional events as needed.**

| Event | Description | Counties | Operation Mode |
| --- | --- | --- | --- |
| *EXAMPLE* | *Example of the table* | *County X, Y, and Z* | *Automatic, manual, delay, etc.* |
| CDW | Civil Danger Warning | | |
| CEM | Civil Emergency Message | | |
| EQW | Earthquake Warning | | |
| EVI | Evacuate Immediate | | |
| FRW | Fire Warning | | |
| HMW | Hazardous Materials Warning | | |
| LAE | Local Area Emergency | | |
| LEW | Law Enforcement Warning | | |
| SPW | Shelter in Place Warning | | |
| TOE | 911 Telephone Outage | | |
| RMT | Required Monthly Test | | |
| RWT | Required Weekly Test | | |
| | | | |
| | | | |

| Does your device re-transmit both 'Description' and 'Instruction' CAP elements? | |
| --- | --- |

| Are you willing to coordinate additional testing from local agencies in the community? | |
| --- | --- |

| Is there any other information the County may need to know? | |
| --- | --- |

# Appendix E – Model WEA Survey Form

The WEA Survey Form can be found on the following page and as an attached Word file.

*The remainder of this page intentionally left blank.*

# WEA Survey

**Carrier:** _____

**24/7 Contact Number:** _____

**County:** _____

**Notes:**

[blank box]

**IPAWS POC:**

**Name:** _____

**Address:** _____

**Phone:** _____

**E-mail:** _____

**Re-transmit Rate:** _____

**Can the re-transmit rate be reduced in critical counties?** _____

**IPAWS Implementation:**

Describe the way IPAWS messages are processed for this county (by FIPS, by coordinates, by polygon coordinates). Do the coordinates have to include the tower latitude/longitude or just the sector?

**Common Tower Information (this should match the E9-1-1 information)**

| County | Carrier Name Field | House Number Field | House Number Suffix | Prefix Directional | Street Field/Name | Street Suffix | Post Directional | Community Field | State (2 char. Max) | Location (20 char. Max) | FIPS Assigned for IPAWS | Cell Tower Latitude (in decimal degrees) (+/- 2 before decimal/6 after decimal) | Cell Tower Longitude (in decimal degrees) (+/- 3 before decimal/6 after decimal) | Cell Sector Orientation/ Azimuth (degrees, N=0) | Cell Sector Beam Width (degrees) | Cell Sector Compass Orientation | Avg. Cell Sector Radius Range (Miles) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |

# Appendix F – Model Alert and Notification Plan

The *Model Alert and Notification Plan* can be found on the following pages and as an attached Word file.

*The remainder of this page intentionally left blank.*

# Model Alert and Notification Plan

# for

# Integrated Public Alert and Warning System (IPAWS)

*April 2014*

In {Jurisdiction}, the Emergency Alert System (EAS) is a system used by the Emergency Operations Center (EOC) to send alerts and notifications. The National Weather Service (NWS) has been the primary user of the technology to send severe weather warnings over its National Oceanic and Atmospheric Administration (NOAA) Weather Radio System. EAS has not seen wide usage at a local level in {State} for many years. EAS responsibilities have been shared by {State} Office of Emergency Management (OEM) EOC, NWS, and the {State} Broadcasters Association since the inception of EAS in the 1990s. Although designed to be a bottom-up system, it has remained a top-to-bottom warning system on a regional and/or statewide basis. Local use has been spotty. Local warning in rural areas with EAS is hampered by the lack of broadcast radio stations. Many jurisdictions do not have a local radio station, and many local stations do not originate their programming. The result is an EAS system that is not local. Integrated Public Alert and Warning System (IPAWS) technology supports local warning.

Historically, the public depended exclusively on radio and television to receive alerts, but current research shows that radio and television reach less than 40 percent of the population during the work day. Less than 12 percent of the population is watching television in the middle of the night, and only 5 percent is tuned to the radio. Television and radio will continue to be valuable sources of public information, but their reach is decreasing. Furthermore, these information sources can only target a state or regional area and do not encompass alerting for people who do not speak English or those with disabilities and other access and functional needs, including the 29 million Americans with hearing impairment.

Today, the Internet and cellular phones are increasingly popular and, therefore, are valuable sources of information. While television remains the most popular source for information, the Internet ranked either first or second at both work and home.

Effective this date in accordance with {authority reference}, the {Agency} Alert and Notification Plan is hereby approved.


_____
Name


_____
Date


_____
Title


_____
Agency

## *Record of Changes*

All changes are to be annotated on the master copy of the IPAWS Implementation Plan. Should the change be significant in nature, updates shall be made to applicable Web pages. If not, changes will be reviewed and incorporated into the plan during the next scheduled update.

| Date Posted | Change | Page / Paragraph / Line | Recommending Agency / Individual |
|---|---|---|---|
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**TABLE OF CONTENTS**

**EXECUTIVE SUMMARY**

The Integrated Public Alert and Warning System (IPAWS) is designed to improve public safety through the rapid dissemination of emergency messages to as many people as possible over as many communications devices as possible. To accomplish this, IPAWS is expanding the traditional Emergency Alert System (EAS) to include more modern technologies. At the same time, the Federal Emergency Management Agency (FEMA) is upgrading the alert and warning infrastructure so that, no matter what the crisis, the public will receive life-saving information.

The advent of new media has brought a dramatic shift in the way the public consumes information. IPAWS capitalizes on multiple electronic media outlets to ensure that the public receives life-saving information during a time of national emergency.

## 1. SITUATION

## 2. AUTHORITY

Authoritative information for this plan is garnered from the following:

- Comprehensive Preparedness Guide 101, November 2010
- Executive Order 13407, Public Alert and Warning System, dated June 26, 2006
- National Incident Management System, December 2008
- National Response Framework (NRF), January 2008
- Post-Katrina Emergency Management Reform Act 2006 (S.3721—109th Congress)
- Robert T. Stafford Relief and Emergency Assistance Act (42 U.S.C. 5121, et seq.)\
- *Insert {State} Statutes related to alert and warning*
- {State} Emergency Operations Plan (EOP)

## 3. PURPOSE

Broadcasting alerts and warning to the population is one of the primary responsibilities of government at all levels. This system began during the Cold War when the threat of nuclear war was high, and it provided a means for the President to address the public. Over time, the system was expanded to cover other threats such as natural disasters (flooding, hurricanes, severe weather, tornados, etc.). Other Federal agencies such as the National Weather Service (NWS) were allowed to broadcast more localized alerts and warnings.

With the rapid growth of new communications methods, the need to upgrade the current EAS was recognized. In 2006, the modernization of the nation's EAS along with integration to other multiple communications pathways for alerting the public was envisioned in Executive Order 13407. The Integrated Public Alert and Warning System (IPAWS) Program Office was established by FEMA in 2007 to implement the vision of the Executive Order. Beginning in 2011, initial IPAWS capabilities were deployed, providing public safety authorities at all levels of government integrated access to send alerts to EAS, the National Oceanic and Atmospheric Administration (NOAA) Weather Radio, a new cellular alerting capability called Wireless Emergency Alerts (WEA), Internet applications, and future alerting channels and communications technologies yet to be developed. IPAWS offers authorities a broader range of message options and multiple communications pathways and increases the capability to alert and warn communities of all hazards that have an impact on public safety.

IPAWS seeks to provide timely alert and warning to American citizens, residents, and visitors in the preservation of life and property. The IPAWS national mission statement identifies the intent:

> *Provide integrated services and capabilities to Federal, State, territorial, tribal, and local authorities that enable them to alert and warn their respective communities via multiple communications methods.*

To successfully accomplish this mission, three program goals have been outlined:

Goal 1:   Create and maintain an integrated interoperable environment for alert and warning
Goal 2:   Make alert and warning more effective
Goal 3:   Strengthen the resilience of IPAWS infrastructure

The IPAWS architecture and associated elements can be found in Appendix A.

Since 2006, several small-scale IPAWS tests and the first ever nationwide EAS test have occurred. The next phase is to expand IPAWS to incorporate State structures through a memorandum of agreement (MOA) that will govern the relationship between State-level Collaborative Operating Groups (COGs) and FEMA.

This Implementation Plan is designed to provide direction and guidance for the integration of IPAWS into existing emergency communication systems with the ultimate objective of becoming the primary system for communicating with the general public during local disasters and/or emergencies or a national-level emergency incident.

## 4.  IPAWS ALERTING PLAN DETAIL

IPAWS messages may be used to alert the public to events that pose a significant threat to life and/or property. **IPAWS is a public <u>warning</u> system, NOT a public <u>information</u> system.** Presidential messages are issued by the President of the United States. AMBER Alerts are issued by State Police. Critical weather warnings are issued by NWS.

Alerts issued by an authorized public safety agency using IPAWS may be directed to three dissemination channels: broadcast media (EAS), weather radios (non-weather emergency messages [NWEM]), and cell phones via WEA. Some alerts may only need to go to one channel; other alerts may go to two or all three channels.

The primary capability of a WEA (cell phone) message is to quickly alert recipients that an event is occurring (or will occur) in the geographic area in which the recipient is located. WEA limits the message to 90 characters at one time.

EAS (broadcasters) and NWEM (weather radio) alerts can provide more information. For example, the "Headline" element of a NWEM message may be 160 characters and the "Description + Instruction" elements may be up to 160 words total. WEA messages are limited to 90 characters of text only. The WEA message content can be entirely composed by the Alerting Authority (using the "CMAMText" element) or may be automatically generated from values in the Common Alerting Protocol (CAP) description, instruction, area description, and alert begin and end time elements as provided in the Alerting Authority's CAP message.

## 4.1. CRITERIA FOR ISSUING IPAWS MESSAGES

When circumstances exist where the need for a public warning becomes necessary, it will ultimately be a matter of local judgment. To assist in the decision-making process, the following criteria can be applied:

- Does the hazardous situation require the public to take immediate action?
- Does the hazardous situation pose a serious threat to life or property?
- Is there a high degree of probability the hazardous situation will occur?
- Are other means of disseminating the information adequate to ensure rapid delivery of urgent information?

The figure below illustrates a decision tree to aid in the decision-making process.
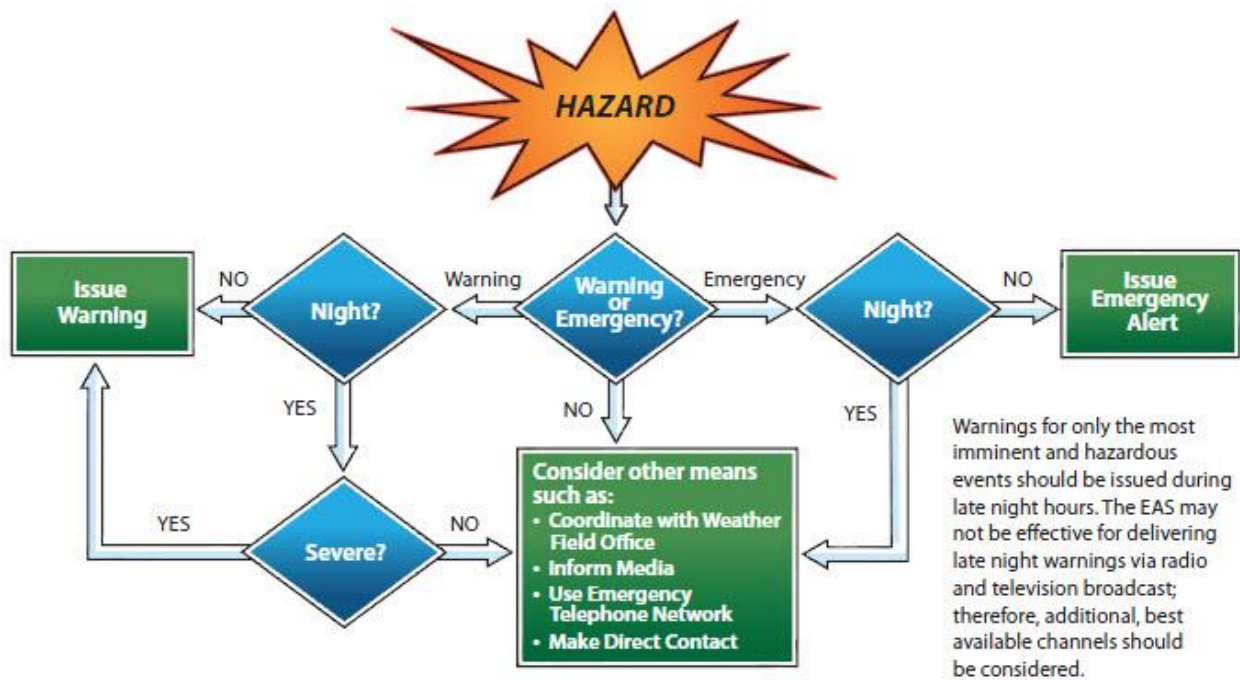


## 4.2. TYPES OF IPAWS MESSAGES

There are two types of alert messages for which emergency management will use IPAWS: warnings and emergencies.

- **Warning messages:** Warning messages are issued for those events that alone pose a significant threat to public safety and/or property, probability of occurrence and location is high, and the onset time is relatively short.

- **Emergency messages:** Emergency messages are issued for those events that by themselves would not kill or injure or do property damage but indirectly may cause other things to happen that result in a hazard.

## 4.3.  TRAINING REQUIREMENTS

Prior to initial access and posting alerts, training requirements for IPAWS are as follows:

- Computer security awareness training prior to initial access and annually thereafter, either a locally delivered course or, if not available locally, Domestic Preparedness Campus online course, CYBER 175-W (175-W) — Information Security for Everyone (https://teex.org/Pages/Class.aspx?course=AWR175&courseTitle=Information%20Security%20for%20Everyone)
- IS-247.a course for COG point of contact (POC) and any user with Alerting Authority for IPAWS public alerts (http://www.training.fema.gov/is/courseoverview.aspx?code=IS-247.a)
  - ο The COG POC must complete IS-247.a and submit a copy of his or her training certificate as part of the application process. All other training records are maintained locally.

## 4.4.  SOFTWARE FOR SENDING ALERTS

A list of system developers, available from the FEMA website, indicate which vendors have completed development or are developing alerting tools for use with IPAWS. (http://www.fema.gov/media-library/assets/documents/25916)

## 4.5.  ACTIVATING ALERTS

The four free-text fields of an alert (Headline, Description, Instructions and CMAMtext [cell phone message]) must be reviewed before posting. Rushed alerts with poor wording can have disastrous effects. Messages should be pre-scripted as much as possible prior to an event.

### 4.5.1.  *Effective Alert and Warning Messages*

How an alert or warning message is written is as important as what is written. Poorly written warnings can undermine both understanding and credibility. "Style" refers to how you write. Considerations when writing accessible and usable alert and warning messages should include:

- Specific: If the message is not specific enough about the who, what, when, where, why, and how of the incident, the public will spend more time seeking specific information to confirm the risk than responding to the message. If necessary, be specific about what is or is not known about the hazard.
- Consistent: An alert or warning message should be internally consistent; that is, one part of the message should not contradict another part. It should be consistent with messages that are

distributed via other channels. To the extent possible, alerts and/or warnings should be consistent from event to event to the degree that the hazard is similar.

- Certain: Avoid conveying a sense of uncertainty, either in content or in tone. Confine the message to what is known or, if necessary, describe what is unknown in certain terms. Do not guess or speculate.
- Clear: Use common words that can easily be understood. Do not use technical terminology or jargon. If protective instructions are precautionary, state so clearly. Make it clear if protective instructions pertain to particular at-risk populations (e.g., elderly). If the probability of occurrence of the hazard event is less than 100 percent, try to convey in simple terms what the likelihood of occurrence is.
- Accurate: Do not overstate or understate the facts. Do not omit important information. Convey respect for the intelligence and judgment of the public.

To this end, only those individuals who have successfully completed the IS-247.a course and have been officially designated by their jurisdiction as an Alerting Authority will be provided access to the system. FEMA will approve the State-designated POC. This POC will then be responsible for verifying and certifying applicable State agency, local jurisdiction, and tribal government Alerting Authorities within the State.

## 4.6. SYSTEM SECURITY

To ensure joint security of the systems and the message data they store, process, and transmit, all parties participating in IPAWS agree to the following:

- Authorized users accessing the interoperable system(s) receive, agree to abide by, and sign (electronically or in paper form) the IPAWS-Open Platform for Emergency Networks (IPAWS-OPEN) Rules of Behavior. Each jurisdiction is responsible for keeping the signed Rules of Behavior on file or stored electronically for each system user.
- FEMA-approved public key infrastructure (PKI) certificates must be used to digitally sign messages as they are transported over the public Internet.
- Each jurisdiction must certify that its respective system is designed, managed, and operated in compliance with all relevant Federal laws, regulations, and policies.
- Each jurisdiction must document and maintain jurisdictional and/or system-specific security policies and procedures and produce such documentation in response to official inquiries and/or requests.
- Each jurisdiction must provide physical security and system environmental safeguards for devices supporting system interoperability with IPAWS.
- Where applicable, only individuals who have successfully completed FEMA-required training can use the interoperable systems to issue alerts and warnings intended for distribution to the public.
- Where applicable, records of successful completion of FEMA-required training must be documented and maintained, and such documentation must be produced in response to official inquiries and/or requests.

- All e-mail addresses provided in connection with interoperable system(s) user accounts are associated to an approved e-mail account assigned by the user's emergency management organization. The use of personal e-mail accounts to support emergency messaging through IPAWS is prohibited.
- Upon approval of the MOA by FEMA, a COG account with a COG identification (ID) number and digital certificate will be created and issued to the designated technical representative. All individuals with knowledge of these credentials must not share or alter these authentication mechanisms without explicit approval from IPAWS.
- Physical and logical access to the respective systems, as well as knowledge of the COG ID and associated access criteria, are only granted to properly vetted and approved entities or individuals.
- Every interoperable system user is responsible for remote access security as it relates to his or her use of IPAWS and shall abide by the Rules of Behavior per COG MOA.
- All users must have a discrete user account ID, which cannot be the user's social security number. To protect against unauthorized access, passwords linked to the user ID are used to identify and authenticate authorized users.
- Accounts and passwords shall not be transferred or shared. The sharing of both a user ID and associated password with anyone (including administrators) is prohibited.
- Accounts and passwords shall be protected from disclosure, and writing passwords down or electronically storing them on a medium that is accessible by others is prohibited.
- The selection of passwords must be complex and include:
  ο At least eight characters in length
  ο At least two uppercase and two lowercase letters
  ο At least two numbers and one special character
- Passwords must not contain names, repetitive patterns, dictionary words, product names, or personal identifying information (e.g., birthdate, social security number, phone number) and must not be the same as the user ID.
- Users are required to change their passwords at least once every 90 days.
- Passwords must be promptly changed whenever compromise of a password is known or suspected.
- All computer workstations accessing IPAWS must be protected by up-to-date antivirus software. Virus scans must be performed on a periodic basis and when notified by the antivirus software.
- Users accessing interoperable systems to use IPAWS must:
  ο Physically protect computing devices such as laptops, personal electronic devices, BlackBerry® devices, smart phones, etc.;
  ο Protect sensitive data sent to or received from IPAWS;
  ο Not use peer-to-peer (P2P) file sharing, which can provide a mechanism for spreading viruses and put sensitive information at risk; and
  ο Not program computing devices with automatic sign-on sequences, passwords or access credentials when using IPAWS.
- Users may not provide personal or official IPAWS information solicited by e-mail. If e-mail messages are received from any source requesting personal information or asking to verify

accounts or other authentication credentials, users must immediately report this and provide the questionable e-mail to the local System Administrator and/or the State POC.

- Only devices officially issued through or approved by the U.S. Department of Homeland Security (DHS), FEMA, and/or approved emergency management organizations are authorized for use with IPAWS.
- If a BlackBerry®, smart phone, or other personal electronic device is used to access the interoperable system(s) to use IPAWS, the device should be password-protected and configured to timeout or lock after 10 minutes of inactivity.
- If sensitive information is processed, stored, or transmitted on wireless devices, it must be encrypted using approved encryption methods.

## 4.7. SYSTEM TESTS

At the local, county, and State level, quarterly tests or exercises of IPAWS will be conducted to ensure the ability to send emergency notification information across the entire network. Any impediments will be immediately identified and a resolution at the lowest jurisdictional level possible will be ascertained.

It is anticipated that the FEMA IPAWS Program Management Office (PMO) will conduct tabletop, scenario-based, and full–scale exercises of the public alert and warning communication systems. Where applicable, all jurisdictions will be encouraged to participate in these exercises. Additionally, the State and/or local jurisdictions may find it necessary to conduct IPAWS-only exercises to test the connectivity of the network. Though these exercises may involve a small portion of the response community, they do need to be reflected on the State's regionally defined Training and Exercise Planning Workshop (TEPW) calendars. If an IPAWS component is to be part of a larger exercise, then it does not need to be included on a TEPW calendar.

## 4.8. COORDINATION

### 4.8.1. Local Media

Local media has a desire to keep their audiences informed of ongoing events. Besides their broadcasts, many have developed instant messaging systems to keep the public informed of key events through a variety of social media networks. Coordination with local media outlets is one of the linchpins to successfully communicating alerts to the public through IPAWS. Making use of media's desire to inform its audience, jurisdictions have established and continue to build relationships with the media for the passage of critical, time-sensitive information.

The challenge is that many media outlets are market-driven and are not constrained by political boundaries. In many cases, a television or radio broadcast station that covers multiple counties/localities or State-defined regions may be physically located in a neighboring State.

### 4.8.2. *Public*

Public outreach will primarily be in two forms. First, through multiple venues, such as newspaper articles, public service announcements, town hall meetings, or other activities that the jurisdiction has found effective, the general public will be encouraged to continue to listen to and follow officials' guidance as to what to do when a disaster occurs.

Second, periodically (especially after an incident occurs) the public should be canvassed as to the clarity and effectiveness of the messages that were broadcast. The responses should be reviewed to determine if any changes to the message content need to take place. The results should also be passed to the applicable State agency to share for the benefit of other jurisdictions.

## 5. ROLES AND RESPONSIBILITIES

### 5.1. FEDERAL

FEMA is the lead Federal agency for IPAWS coordination and implementation. FEMA ensures that the system is functional, maintained, and tested to achieve the following:

- Build and maintain an effective, reliable, integrated, flexible, and comprehensive alert and warning system.
- Enable Federal, State, territorial, tribal, and local alert and warning emergency communication officials to access multiple broadcast and other communications pathways for the purpose of creating and activating alert and warning messages related to hazards impacting public safety and well-being.
- Reach the American public before, during, and after a disaster through as many means as possible.
- Diversify and modernize the EAS.
- Create an interoperability framework by establishing or adopting standards such as CAP.
- Enable alert and warning to those with disabilities and others with access and functional needs and to those without an understanding of the English language.
- Partner with NOAA to enable seamless integration of message transmission through national networks.
- Receive and authenticate alert messages, then simultaneously deliver to all IPAWS–compliant public alerting systems.
- Continue to engage the media, Internet service providers, unique and local alerting system providers, and future alert technology developers on the implementation of IPAWS.
- Authenticate State-level Alerting Authorities.
- Allow the President of the United States to speak to the American people under all emergency circumstances, including situations of war, terrorist attack, natural disaster, or other hazards.
- Ensure the required Emergency Management Institute (EMI) courses are available and updated periodically.

## 5.2. STATE

Recognizing that all disasters are local, the primary responsibility of the State will be to facilitate the implementation of IPAWS into the emergency notification network. In the case of a catastrophic local/State or regionally-defined event, the State will use IPAWS to provide a resilient and comprehensive alert and notification capability.

- The {State} Office of Emergency Management (OEM) will be designated the COG as per the signed MOA with FEMA.
- _____ shall be the alternate State agency to provide statewide IPAWS warnings and alerts.
- OEM will form a working group comprising applicable statewide stakeholders. This working group will bring together the necessary technical and operational expertise from the private sector, nonprofit organizations, local jurisdictions, State agencies, and the Federal government with the goal of defining policy and procedures leading to the implementation of IPAWS across the State. The working group shall include representatives from the following agencies:
  - o OEM
  - o {State} Broadcasters Association
  - o NWS
  - o A representative from the Commercial Mobile Radio Service (CMRS) Emergency Telecommunications Board (Board)
  - o Representatives from local Emergency Management Agencies (EMAs)
  - o A representative from the State Emergency Response Commission
- OEM will be the authentication source for all local and State agency Alerting Authorities.
- OEM will track approved COGs.
- OEM will be the approving agent for local jurisdictional requests and/or plans to incorporate locally contracted providers into the IPAWS network.
- OEM will conduct periodic tests of the system to ensure functionality of equipment and the network.
- OEM will provide a backup capability for local jurisdictions' Alerting Authorities to issue emergency broadcasts in the name of the local jurisdiction.

## 5.3. LOCAL JURISDICTIONS

Except in rare occurrences such as the events of September 11, 2001, most disasters and emergencies are locally oriented. While first responders gear up to respond to the initial aftereffects of an incident, it is an inherent responsibility of local officials to keep the public informed of what actions the public needs to take to protect themselves from the consequences of the incident. These could include evacuation orders, location of points of distribution (for food, water, drugs, etc.), instructions to move to higher ground, shelter-in-place guidance and orders to take cover. Passing these instructions to the public is the primary purpose of IPAWS. Because local officials have a better understanding of

the situation, the immediate actions that are being taken, and potential adverse impacts of the incident, it is incumbent upon these officials to rapidly and effectively communicate to the public what is going on and what needs to be done.

To successfully accomplish this task, local jurisdictions need to have a structure in place to provide for this rapid alert and warning. Many of the tasks leading to this structure will include the following:

- Submit to the State a request and/or plan that identify emergency notification providers/systems for inclusion into the IPAWS network.
- Designate in writing, in accordance with jurisdictional procedures, no fewer than three individuals who will be the jurisdiction's Alerting Authorities for issuing emergency broadcasts with IPAWS following their successful completion of IS–247.a – **Integrated Public Alert and Warning System (IPAWS)** course. Typically, this would be the jurisdiction's emergency manager and staff.
- Incorporate IPAWS into existing and future response plans and procedures as well as training and exercise events.
- Conduct periodic tests of the system to ensure functionality of equipment and the network.

COGs will maintain a database of all individuals who have successfully completed the IS-247.a course and other required courses as directed by Federal guidance. This database will contain copies of completed course certificates; individual names, addresses, and contact information; and copies of memorandums and/or resolutions officially designating these individuals as Alerting Authorities. A copy of each jurisdiction's signed Rules of Behavior will also be included.

COG-level permissions must be obtained from NWS to submit NWEMs via NOAA weather radio.

Immediately after broadcast, a copy of the alert must be sent (COG to COG, faxed, or e-mailed) to the State OEM, and the County Judge/Executive or Mayor (Statutory authority) must be notified.

## 6. PLAN MAINTENANCE

This Plan shall be maintained and kept current by all parties on the following schedule:

- Updates can occur at any time based upon the change of Federal guidance.
- A cursory review of the Plan will be performed on an annual basis. Changes will be annotated on the Record of Change sheet.
- A complete review and update of the Plan will occur every 4 years at a minimum. This review will consist of all partners having the opportunity to comment on all elements of the Plan.

Review and revision of procedures will follow critiques of actual emergency or disaster operations and/or exercises where deficiencies were noted.

# Acronyms

| | |
|---|---|
| CAP | Common Alerting Protocol |
| CMAS | Commercial Mobile Alert System |
| COG | Collaborative Operating Group |
| CMRS | Commercial Mobile Radio Service |
| EAS | Emergency Alert System |
| EMI | Emergency Management Institute |
| EOC | Emergency Operations Center |
| FEMA | Federal Emergency Management Agency |
| FIPS | Federal Information Processing Standard |
| ICS | Incident Command System |
| IPAWS | Integrated Public Alert and Warning System |
| OEM | Office of Emergency Management |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |
| NOAA | National Oceanic and Atmospheric Administration |
| NWEM | Non-Weather Emergency Message |
| NWS | National Weather Service |
| OPEN | Open Platform for Emergency Networks |
| PKI | Public Key Infrastructure |
| POC | Point of Contact |
| TEPW | Training and Exercise Planning Workshop |

# Glossary

**Agency Representative**—A person assigned by a primary, assisting, or cooperating Federal, State, local, or tribal government agency or private entity that has been delegated authority to make decisions affecting that agency's or organization's participation in incident management activities following appropriate consultation with the leadership of that agency.

**Agency**—A division of government with a specific function offering a particular kind of assistance. In the Incident Command System (ICS), agencies are defined either as jurisdictional (having statutory responsibility for incident management) or as assisting or cooperating (providing resources or other assistance).

**Alerting Authority**—Designated jurisdictional individual who is authorized to write an alert or warning for distribution using open standards and to release the alert or warning.

**Collaborative Operating Group**—IPAWS is structured around COGs. A COG is a virtual organization that holds membership in IPAWS and manages system access within that organization. When the application process is complete, FEMA will assign each agency a COG ID number and digital certificate.

**Disaster** (State Definition)—*The occurrence or imminent threat of widespread or severe damage, injury, or loss of life or property, or significant adverse impact on the environment, resulting from any natural or technological hazards, or a terrorist act,* including fire, flood, earthquake, wind, storm, hazardous substance incident, water contamination requiring emergency action to avert danger or damage, epidemic, air contamination, blight, drought, infestation, explosion, civil disturbance, and hostile military or paramilitary action. For the purpose of State or Federal disaster declarations, the term "disaster" generally falls into one of two categories relative to the level of severity and impact on local and State resources. They are: Major (i.e., likely to require immediate State assistance supplemented by limited Federal resources, if necessary, to supplement intra-state efforts and resources) and Catastrophic (i.e., - will require immediate and massive State and Federal assistance in both the response and recovery aspects). Local government's adaptation of the definition of a disaster denotes an event that threatens to or actually does inflict damage to people or property and is or is likely to be beyond the capability of services, personnel, equipment, and facilities of a local jurisdiction, thereby requiring augmentation of resources through State-directed assistance.

**Emergency** (State Definition)—*A suddenly occurring and often unforeseen situation* that is determined by the Governor to require State response or mitigation actions to immediately supplement local government in protecting lives and property, to provide for public health and safety, or to avert or lessen the threat of a disaster. Local government's adaptation of this definition connotes an event that threatens to or actually does inflict damage to people or property, exceeds the daily routine type of response, and still can be dealt with using local internal and mutual aid resources.

**Integrated Public Alert and Warning System (IPAWS)**—In the event of a national emergency, the President will be able to use IPAWS to send a message to the American people quickly and simultaneously through multiple communications pathways. IPAWS is also being made available to Federal, State, local, territorial, and tribal government officials as a way to alert the public via EAS, WEA, NOAA Weather Radio and other NWS dissemination channels, the Internet, existing unique warning systems, and emerging distribution technologies.

**Jurisdiction**—A range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority for incident mitigation. Jurisdictional authority at an incident can be political or geographical (e.g., city, county, State, or Federal boundary lines) or functional (e.g., police department, health department).

**Memorandum of Agreement (MOA)**—An agreement document between two or more agencies proscribing reciprocal assistance to be provided upon request (and if available from the supplying agency) and laying out the guidelines under which this assistance will operate.

**Memorandum of Understanding (MOU)**—A non-reimbursable agreement between two or more agencies.

**Mutual-Aid Agreement**—A written agreement between agencies and/or jurisdictions indicating that they will assist one another on request by furnishing personnel, equipment, and/or expertise in a specified manner.

**National Weather Services (NWS)**—Federal government agency charged with weather-related reporting and projections.

**Shelter in place**—A course of action to take immediate shelter where you are—at home, work, school, or wherever you can take protective shelter. It may also mean "seal the room," i.e., take steps to prevent outside air from coming in.

**State**—When capitalized, refers to any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States. See Section 2 (14), Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002).

# Appendix A: IPAWS Architecture and Alert Elements

## IPAWS Architecture

*Standards Based Alert Message protocols, authenticated alert message senders, shared, trusted access & distribution networks, alerts delivered to more public interface devices*
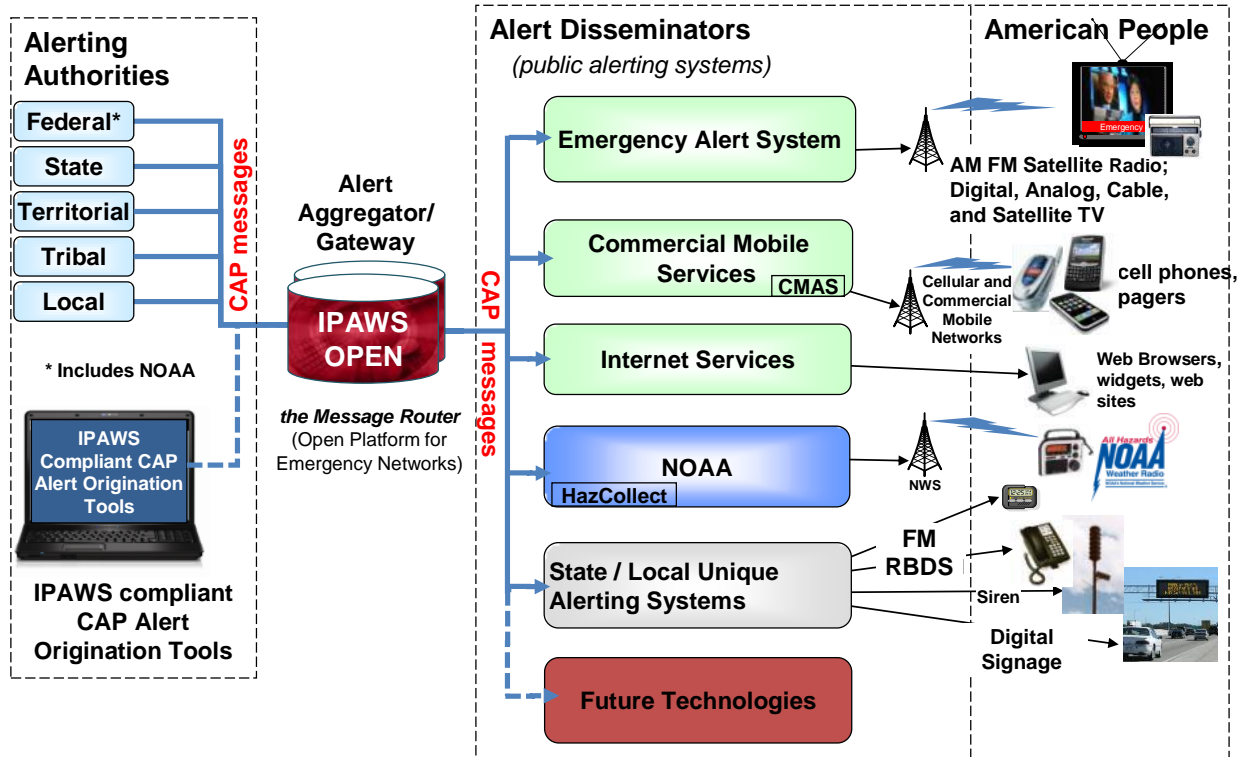


## Alert Elements

**Event Codes that will pass all three dissemination channels:**

| | |
|---|---|
| CDW | Civil Danger Warning |
| CEM | Civil Emergency Message |
| EQW | Earthquake Warning |
| EVI | Evacuate Immediate |
| FRW | Fire Warning |
| HMW | Hazardous Materials Warning |
| LAE | Local Area Emergency |
| LEW | Law Enforcement Warning |
| RNW | Radiological Hazard Warning |
| SPW | Shelter in Place Warning |

**Additional Event Codes that may be needed, but will not pass to all three dissemination channels:**

TOE             911 Telephone Outage Emergency (will not go to WEA)
RMT             Required Monthly Test (will not go to NWEM or WEA)
RWT             Required Weekly Test (will not go to WEA)


**CAP Data Info Elements Special Note for Generating WEA:**

The following CAP Info Elements for Urgency Severity and Certainty must each be set to one of the two highest levels to indicate that the alert is an "Imminent Threat," which then enables the alert to be sent as a WEA. The values are set by the Alerting Authority generating the message based upon his or her analysis of the threat at the time that the message is being written:

URGENCY:    Available values for WEA "imminent threat" alert are:
            "Immediate"   Responsive action should be taken immediately
            "Expected"    Responsive action should be taken soon (within next hour)

            Other available values URGENCY that do not qualify a message for WEA are:
            "Future"      Responsive action SHOULD be taken in the near future
            "Past"        Responsive action is no longer required
            "Unknown"     Urgency not known


SEVERITY:   Available values for WEA "imminent threat" alert are:
            "Extreme"     Extraordinary threat to life or property
            "Severe"      Significant threat to life or property

            Other available values' SEVERITY that do not qualify a message for WEA are:
            "Moderate"    Possible threat to life or property
            "Minor"       Minimal to no known threat to life or property
            "Unknown"     Severity unknown


CERTAINTY:  Available values for WEA "imminent threat" alert are:
            "Observed"    Determined to have occurred or to be ongoing
            "Likely"      Probability is greater than or equal to 50 percent

            Other available values' CERTAINTY that do not qualify a message for WEA are:
            "Possible"    Possible but not likely (p <= ~50 percent)
            "Unlikely"    Not expected to occur (p ~ 0)
            "Unknown"     Certainty unknown

## Event Category

**Event categories include the following:**

| | |
|---|---|
| Geo | Geophysical (including landslides) |
| Met | Meteorological (including floods) |
| Safety | General emergency and public safety |
| Security | Law enforcement, military, homeland and local/private security |
| Rescue | Rescue and recovery |
| Fire | Fire suppression and rescue |
| Health | Medical and public health |
| Env | Pollution and other environmental |
| Transport | Public and private transportation |
| Infra | Utility, telecommunication, other non-transport infrastructure |
| CBRNE | Chemical, biological, radiological, nuclear or high-yield explosive threat or attack |
| Other | Other events |

**Expires:** A required element for all alerts.

**Headline:** A brief headline less than 140 characters. (Not used by WEA or EAS, but used by NWEM.)

**Description:** A text description of the hazard or event. (Not used by WEA, but used by EAS and NWEM.)

**Instruction:** The recommended action to be taken by recipients of the alert message. (Not used by WEA, but used for EAS and NWEM.)

For NWEM alerts, description and instruction must not exceed 160 words. For EAS alerts, FCC required text and description and instruction combined must not exceed 1,800 characters (where FCC required text is automatically generated by the broadcaster's EAS device).

1. Response Type
   Response type elements used by WEA are as follows:

   | | |
   |---|---|
   | Shelter: | Take shelter in place or per instruction |
   | Evacuate: | Relocate per the instruction |
   | Prepare: | Make preparations per the instruction |
   | Execute: | Execute a pre-planned activity identified in instruction |
   | Avoid: | Avoid the subject event as per the instruction |
   | Monitor: | Attend to information sources as described in instruction |

2. Parameters
   Parameters are not identified in IS-247 training but are required by IPAWS applications.

   EAS-ORG    CIV

Timezone      Dependent upon location (Eastern, Central, or Mountain time zones)

CMAMtext    This is the 90-character message used by CMAS that appears on cell phones. Very important. Use maximum length possible to best describe the alert.

3.    Area Description
Text description of affected area. Used by EAS and NWEM.

4.    Geocode
An alert will most likely be countywide. The 6-digit FIPS code for the county will be used. NWEM messages will all be countywide. Some alerting software allows a map polygon or circle to define the alerting area. An alert message will not be limited to the area of an alert, particularly a small one; there will be coverage overlap by cell towers beyond the defined area.

5.    Resource
The optional resource element and related sub-elements offer the ability to incorporate multimedia such as images, audio, and video as attachments.

## Appendix B: {State} Emergency Alert System Plan

Insert copy of the State EAS plan

## Appendix C: Alert and Notification Capabilities

WXXX – AM Radio 570
Broadcast Area: Model City
24/7 Contact Number: (555) 555-1234

WYYY – AM Radio 1460
Broadcast Area: Model County
24/7 Contact Number: (555) 555-1234

WZZZ – FM Radio 102.1
Broadcast Area: Model City
24/7 Contact Number: (555) 555-1234

WXYZ – Television Channel 2
Broadcast Area: Model City
24/7 Contact Number: (555) 555-1234

ABC Wireless
24/7 Contact Number: (555) 555-1234
Model County Cable
24/7 Contact Number: (555) 555-1234

## Appendix D: Use of IPAWS for Pre-planned Events

**Purpose:**
To provide guidelines for the use of IPAWS and distribution media for alerting the public to events that may pose a risk to the public due to pre-planned events.

The use of IPAWS during a pre-planned event may be a viable method to alert the public of the event and mitigate panic and risk to the public and participants. These messages would advise the public of the event and that there is no cause for alarm or warn the public of any risks. This guideline does not supplant the authority of the individual jurisdiction's elected officials and emergency management staff. Any alert must still be approved by the Alerting Authority for the jurisdiction before being sent.

**Planning:**
During the planning of a pre-planned event (exercise or public event), the risks associated with the event should be identified. If the planned event has a potential risk to the public or public safety, the use of IPAWS to mitigate that risk may be appropriate.

Examples of events and risks:

- Controlled burn of large area
  Risks: Smoke on roadway impairing driving, medical conditions of people in area

- Planned power outage
  Risks: Health and media conditions, traffic accidents

- School active shooter exercise
  Risks: Panic of the general public in the area, Good Samaritan reactions putting the players at risk

- Major bicycle road race
  Risks: Traffic accidents, injury to riders and bystanders

During the planning for each event, the Alerting Authority should review the event and identify the risks. These risks should be reviewed against the permitted uses and target audiences of the various IPAWS dissemination media. The Alerting Authority will determine if the use of IPAWS is appropriate. Guidelines for the use of IPAWS should be defined and documented in the event plan or an appendix.

**Authorized Use:**
IPAWS has several dissemination media. Each system has a different audience and rules for use.

| Dissemination System | Audience | Rules | Notes |
|---|---|---|---|
| Emergency Alerting System (EAS) | Broadcast Radio and Television viewers (not internet or satellite) | 47 CFR 11 State EAS Plan | Broadcasters are not required to re-transmit alerts from local authorities. An EAS alert will be delivered to a large audience. |
| Wireless Emergency Alerts (WEA) | Wireless phones in the area of the alert | 47 CFR 10 | WEA has specific criteria for use. See * below. |
| Non-Weather Emergency Messages (NWEM) | Weather radio users | NWS policies | NWEM alerts will be sent to a National Weather Service transmitter that covers a large area. The alert may also be rebroadcast by broadcast radio and television as an EAS message, but the entities are not required to carry. |
| IPAWS All-Hazards Information Feed | Third-party software and service providers; usually a subscription type service | IPAWS rules | Currently, defining specific criteria for delivery due to the many varied systems using this data is unclear. |
| Collaborative Operating Group (COG) to COG | Other specific COGs | IPAWS rules | Used to coordinate and share information between COGs. |

* For an alert to be sent to the WEA system, the event must meet the following criteria in accordance with 47 CFR 10.400:

(1) Urgency. The CAP Urgency element must be either Immediate (i.e., responsive action should be taken immediately) or Expected (i.e., responsive action should be taken soon, within the next hour).

(2) Severity. The CAP Severity element must be either Extreme (i.e., an extraordinary threat to life or property) or Severe (i.e., a significant threat to life or property).

(3) Certainty. The CAP Certainty element must be either Observed (i.e., determined to have occurred or to be ongoing) or Likely (i.e., has a probability of greater than 50 percent).

**Message Format/Content:**
When using IPAWS for a pre-planned event, the Alerting Authority has the ability to write alert messages in advance to properly communicate the message. Using message templates, various expected messages should be developed to use or have available in the event they are needed.

The Alerting Authority must be identified in all alert messages.

Each audience, message, and distribution media should be reviewed. Is the audience smaller than the distribution media will reach? Will the message cause more concern to the public than the event? Below are some general guidelines for using the available distribution media.

- It is not recommended that the Alerting Authority use WEA messages unless the Alerting Authority has the ability to include and edit the free-form 90 character <CMAMText> element into the CAP message.

- The WEA message will also allow the Alerting Authority to make effective use of the <expires> element to keep alerts active for the time of the event. WEA messages, unlike EAS, will be broadcast to phones as they enter the selected area of the alert until the <expire> time.

- EAS alerts will be distributed to the broadcast audience, which is often larger than the intended audience. For an event that is small and limited to a specific area, EAS may not be the best distribution media. Understanding how your local broadcast stations are configured is important in selecting the proper distribution media.

- NWEM is also sent to a transmitter that has a large coverage area. The users can use Specific Area Message Encoding (SAME) technology to limit this area, but this will still alert an entire county. In some cases, local broadcast media will monitor the NWEM feed and rebroadcast alerts as an EAS message.

- When determining the event code to use, the following definitions of some common codes from the NWS Instruction 10-518 *Non-weather Related Emergency Products Specifications* are provided to assist in compiling the alert message.

  **Civil Danger Warning (CDW).** A warning of an event that presents a danger to a significant civilian population. The CDW, which usually warns of a specific hazard and gives specific protective action, has a higher priority than the Local Area Emergency (LAE). Examples include contaminated water supply and imminent or in-progress military or terrorist attack. Public protective actions could include evacuation, shelter in place, or other actions (such as boiling contaminated water or seeking medical treatment).

  **Civil Emergency Message (CEM).** An emergency message regarding an in-progress or imminent significant threat(s) to public safety and/or property. The CEM is a higher priority message than the Local Area Emergency (LAE), but the hazard is less specific than the Civil Danger Warning (CDW).

  **Local Area Emergency (LAE).** An emergency message that defines an event that, by itself, does not pose a significant threat to public safety and/or property. However, the event could escalate, contribute to other more serious events, or disrupt critical public safety services. Instructions, other than public protective actions, may be provided by authorized officials.

Examples include a disruption in water, electric or natural gas service, or a potential terrorist threat where the public is asked to remain alert.

**Law Enforcement Warning (LEW).** A warning of a bomb explosion, riot, or other criminal event (e.g., a jailbreak). An authorized law enforcement agency may blockade roads, waterways, or facilities; evacuate or deny access to affected areas; and/or arrest violators or suspicious persons.[18]

**Procedure:**
When using IPAWS for a pre-planned event, the following procedures should be followed:

1. Determine the need.
   a. Determine the event and expected outcomes.
   b. Determine the risks involved.
   c. Determine the benefit that IPAWS can bring to mitigating these risks.

2. Determine whether the use of IPAWS is a benefit and is permitted. (Alerting Authority determines that the use is appropriate given the risk and benefits.)
   a. Incorporate IPAWS into the planning process.
   b. Develop message templates.

3. Coordinate with other jurisdictions and public and private partners.
   a. Notify surrounding jurisdictions of the plan.
   b. Notify the State of the plan.

4. Execute the plan.
   a. Follow the plan for the use of IPAWS.
   b. Notify surrounding jurisdictions when it is activated.
   c. Notify the State when it is activated.
   d. Notify all parties of any changes in the plan.
   e. Notify all parties when event is completed.

---

[18] National Weather Service, Operations and Services; Public Weather Services, NWSPD 10-5, *Non-Weather Related Emergency Products Specification* (Instruction 10-518, July 28, 2010)

# Appendix G – Model MOU Template

The MOU Template can be found on the following pages and as an attached Word file.

*The remainder of this page intentionally left blank.*

# Model Memorandum of Understanding
# for
# Emergency Alerting to the Public

## 1    Introduction

The jurisdictions of [insert counties or jurisdiction names here] recognize the need for interagency cooperation to enhance public-alerting capabilities. This memorandum of understanding (MOU) allows the jurisdictions to improve their ability to warn the public of emergencies in a timely manner where a multi-jurisdictional impact is likely.

## 2    Purpose

This MOU will allow emergency notifications to reach those affected by an incident and help to eliminate duplicate or conflicting instructions. Each jurisdiction participating in this MOU can activate the Integrated Public Alert and Warning System (IPAWS) in an emergency.

## 3    Scope

This MOU is effective as of [Month Day, Year] and will continue until revoked by all parties following the procedures listed in Section 7—Changes to MOU. The MOU may be used when there is an incident other than a weather event that has occurred in a jurisdiction that may impact an area outside of the incident jurisdiction and the incident may impact the outside jurisdiction within 30 minutes.

Parties to the MOU are:

Jurisdiction:
Point of Contact:
Address:
City, State Zip:
E-mail:
Office phone:
24 x 7 phone:
Event Codes Allowed:
FIPS Code:

Jurisdiction:
Point of Contact:
Address:
City, State Zip:
E-mail:
Office phone:
24 x 7 phone:
Event Codes Allowed:
FIPS Code:

# 4      Acronyms and Definitions

"FEMA"—Federal Emergency Management Agency

"IPAWS"—Integrated Public Alert and Warning System

"Memorandum of Understanding" or "MOU"—an agreement between two or more parties for the purpose of formalizing an agreed-upon process or procedure

# 5      Policy

All parties agree that, in the event of an emergency incident that meets the criteria below, the jurisdiction where the emergency originated can initiate an alert for any participating jurisdiction to this MOU.

Incident Criteria:
- The event is not a weather emergency. (National Weather Service will lead these incidents.)
- The incident will impact people outside of the incident jurisdiction within 30 minutes of the onset.
- The incident's impact to people outside of the jurisdiction may be endangered if action is not taken by the public (such as evacuation or shelter in place),
- Jurisdiction A may alert for limited areas of the following jurisdictions:
  ο   Jurisdiction B (FIPS 12345)
  ο   Jurisdiction C (FIPS 23456)
- Jurisdiction B may alert for limited areas of the following jurisdictions:
  ο   Jurisdiction A (FIPS 34567)
  ο   Jurisdiction C (FIPS 23456)
- A message is limited to the following event codes:
  ο   CDW—Civil Danger Warning
  ο   EVI—Evacuate Immediate
  ο   FRW—Fire Warning
  ο   HMW—Hazardous Materials Warning
  ο   SPW—Shelter in Place

Alerts to other jurisdictions will be limited to the geographic area affected, not an entire county or FIPS code.

# 6       Procedures

The originating jurisdiction will use the following procedures:

1) Identify an incident that may impact neighboring jurisdictions.
2) Determine if that impact meets the policy of this MOU.
3) Compose an IPAWS message that includes the other affected jurisdictions' geographic area.
4) Send the IPAWS message.
5) Contact affected jurisdictions to provide detailed information on the incident.
6) Coordinate further alerts with all affected jurisdictions.

The affected jurisdiction will use the following procedures:

1) Monitor IPAWS feeds for all incidents or messages for the jurisdiction.
2) Coordinate with originating jurisdiction for any ongoing alerts or follow up messages.

# 7       Changes to MOU

This MOU will be reviewed and reaccepted each year in January. The originating jurisdiction will send notification to each party to the MOU that the MOU has been reviewed and notification of changes requested.

If changes are requested to this MOU, the requesting jurisdiction will submit the requested changes to all other parties. Each party will review and provide acceptance, modification, or rejection to the originating jurisdiction. If all parties agree to the change(s), the originating jurisdiction will prepare a new version of the MOU for signature by all parties.

If a jurisdiction elects to revoke the MOU, the jurisdiction will notify all other parties of the MOU in writing with a 30-day notice. Each other party will notify its intent to remain a party to the MOU. Remaining parties can continue the MOU in areas that do not pertain to the jurisdiction that has left the MOU. The jurisdiction wishing to revoke the MOU will prepare a new version without their jurisdiction's participation for signature by the other parties. The MOU is fully revoked when there is only one or no party remaining.

The State needs to be notified of any changes to the MOU, including changes of participants. A completed copy of the MOU will be forwarded to the State and to the Federal Emergency Management Agency (FEMA) IPAWS Program Management Office.

# Appendix H – Model Procedures

The Model Procedures can be found on the following pages, and as an attached Word file.

Additional example procedures can be located at the following websites.

**Nebraska**
http://www.nema.ne.gov/pdf/ipaws_seop.pdf

**Michigan Information Letter**
http://www.michigan.gov/documents/msp/IPAWS_Informational_Letter_2-4-13_410325_7.pdf

**Massachusetts**
http://www.mass.gov/eopss/docs/mema/emd-advisory-committee/local-em-program-guidebook.pdf

http://www.mass.gov/eopss/docs/mema/emd-advisory-committee/appendix-a/local-declaration-of-emergency/mema-local-standard-operating-procedure-sop-guidance.doc

**California State University, San Bernardino (Phone Tree)**
http://policies.csusb.edu/emergplan.htm

**Arizona**
http://www.dem.azdema.gov/logistics/docs/comm/CommPlan_Sept08.pdf

**The Homeland Security Digital Library (HSDL)**
This site includes information available to the general public as well as a secure section for public safety.
http://www.hsdl.org/

# Central County
## Standardized Operational Guidelines

**Page X of X**

**Number: 101**

Subject: **Alerting Authority Guidelines**

Approved By: _____       Version #: **2**

Effective Date: **01-01-2013**

Version Date: **01-01-2014**

### Purpose:
Alert authority guidelines define the people and positions with the authority to issue an alert to the public using the alerting systems of Central County.

### Scope:
This guideline applies to staff and volunteers of Central County and all subordinate political jurisdictions for the use of Central County public alerting systems.

### Guidelines:
Statutory authority

State statute XX.YY.ZZ provides that the County Judge has the authority to "provide for the safety and security of the residents of the county." The safety of the county encompasses public alert and notification. The County Judge has determined that other specialists in emergency management and public safety are trained to provide public alerts and notifications. The County Judge has delegated the authority to distribute public alerts and notifications.

Authorized to send alerts:

The following are authorized to operate and distribute public alerts and notifications following Central County guidelines:

- Director of Emergency Management
- Assistant Director of Emergency Management
- Central County Sheriff
- 9-1-1 Director
- On-duty 9-1-1 shift supervisor

Authorized to request alerts:

The following positions are authorized to request public alerts and notifications be distributed:

- Central County Chief Deputy Sheriff
- Anytown Police Chief
- Anytown Assistant Police Chief
- Anytown Fire Chief

- Eastern VFD Fire Chief
- Western VFD Fire Chief
- Incident Commander of an event with more than one agency on-scene

Any authorized requestor will contact the 9-1-1 center to request an alert. The 9-1-1 center will process the request, but the request must be approved by an authorized sender prior to being sent to the public.

# Central County
## Standardized Operational Guidelines

**Number: 102**

**Subject: Alerting System Selection Guidelines**

**Effective Date: 01-01-2013**

**Approved By: _____**     **Version #: 2**     **Version Date: 01-01-2014**

**Purpose:**

System selection guidelines provide guidance for alerting operators to select the appropriate system. Alert and notification systems vary in terms of the time they take to disseminate messages and their effective coverage area. Users should select the appropriate systems based on two critical event-specific characteristics: onset and impact area.

**Scope:**

This guideline applies to staff and volunteers of Central County and all subordinate political jurisdictions for the use of Central County public alerting systems.

**Guidelines:**

The requesting authority will examine the available information regarding current and expected changes of an emergency. The requesting authority will determine the onset and impact area expected to be alerted.

Onset is the maximum time required to deliver a message to the public once an event occurs before adverse impact to that public. Onset is organized into the following categories:

- 0 to 20 minutes
- 21 to 60 minutes
- Hours
- Days

The impact area is the geographic region affected by an event and requiring coverage by an alert. This may be larger than the current area based on expected expansion of the event (e.g., wildfire). When selecting a system, over-alerting (i.e., extending alert coverage beyond the impact area) is typically preferable to under-alerting, but over-alerting can also lead to the public ignoring future alerts. Impact area is organized into the following categories:

- Localized Event: An event (e.g., a sinkhole) that affects a few blocks
- Community-wide Event: An event (e.g., a hazmat incident) that affects all or a major part of a single jurisdictional area

- Multi-community Event: An event (e.g., a tornado) that affects several communities within an area
- Regional Event: An event (e.g., a major flood) that affects an area encompassing many communities and requires assistance from state-level entities

Multi-community and regional events often involve multiple jurisdictions. For these events, alert and notification planning requires the use of the National Incident Management System (NIMS) to direct response and coordinate messaging for single events between jurisdictions. This type of collaborative effort could be undertaken, for example, by a unified command.

The following table can be used by the alerting user to select the appropriate systems. Users may have additional reports from other requestors and should use their best judgment in selecting the proper systems and area to alert. Alerting everyone every time is not a viable option.

| Area ➡ \| System ⬇ | Localized | | | | Community-wide | | | | Multi-community | | | | Regional | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Onset ➡ | 0 – 20 minutes | 21 – 60 minutes | Hours | Days | 0 – 20 minutes | 21 – 60 minutes | Hours | Days | 0 – 20 minutes | 21 - 60 minutes | Hours | Days | 0 – 20 minutes | 21 - 60 minutes | Hours | Days |
| Sirens | ✓ | | | | ✓ | | | | | | | | | | | |
| Public Address | ✓ | ✓ | | | ✓ | ✓ | | | | | | | | | | |
| Radio Alerting Systems | ✓ | | | | ✓ | | | | | | | | | | | |
| Traffic Information and Control Systems | | | | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |
| Legacy Emergency Alert System (EAS) | | | | | ✓ | ✓ | | | ✓ | ✓ | | | ✓ | ✓ | | |
| Social Media | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |
| Press Release | | | ✓ | ✓ | | | ✓ | ✓ | | | ✓ | ✓ | | | ✓ | ✓ |
| IPAWS – Wireless Emergency Alerts (WEA) | | | | | ✓ | | | | ✓ | | | | ✓ | | | |
| IPAWS - EAS | | | | | ✓ | ✓ | | | ✓ | ✓ | | | ✓ | ✓ | | |
| IPAWS - Public Feed | | | | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |

| Onset → System ↓ | 0 – 20 minutes | 21 – 60 minutes | Hours | Days | 0 – 20 minutes | 21 – 60 minutes | Hours | Days | 0 – 20 minutes | 21 - 60 minutes | Hours | Days | 0 – 20 minutes | 21 - 60 minutes | Hours | Days |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IPAWS – National Weather Radio (NWR) | | | | | ✓ | ✓ | | | ✓ | ✓ | | | ✓ | ✓ | | |
| Other Systems | | | | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |

Note: this table can be populated with check marks (as above); P for primary and S for secondary; or ranked 1 – 2 – 3 as priorities for the user.

Another option is to list which systems to use based on severity of the incident. The following is an example of what New York City uses.

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



NYC OEM's Communication Pathways Ranked by Severity
*[adapted from NYC OEM 2012]*

# Central County
## Standardized Operational Guidelines

**Page X of X**

Number: **103**

Subject: **Alerting System Timeframe  Guidelines**          Effective Date: **01-01-2013**

Approved By: _____          Version #: **2**          Version Date: **01-01-2014**

### Purpose:
System timeframe guidelines provide guidance to alerting operators for when to use the appropriate system. Various systems are best used during certain times of the day.
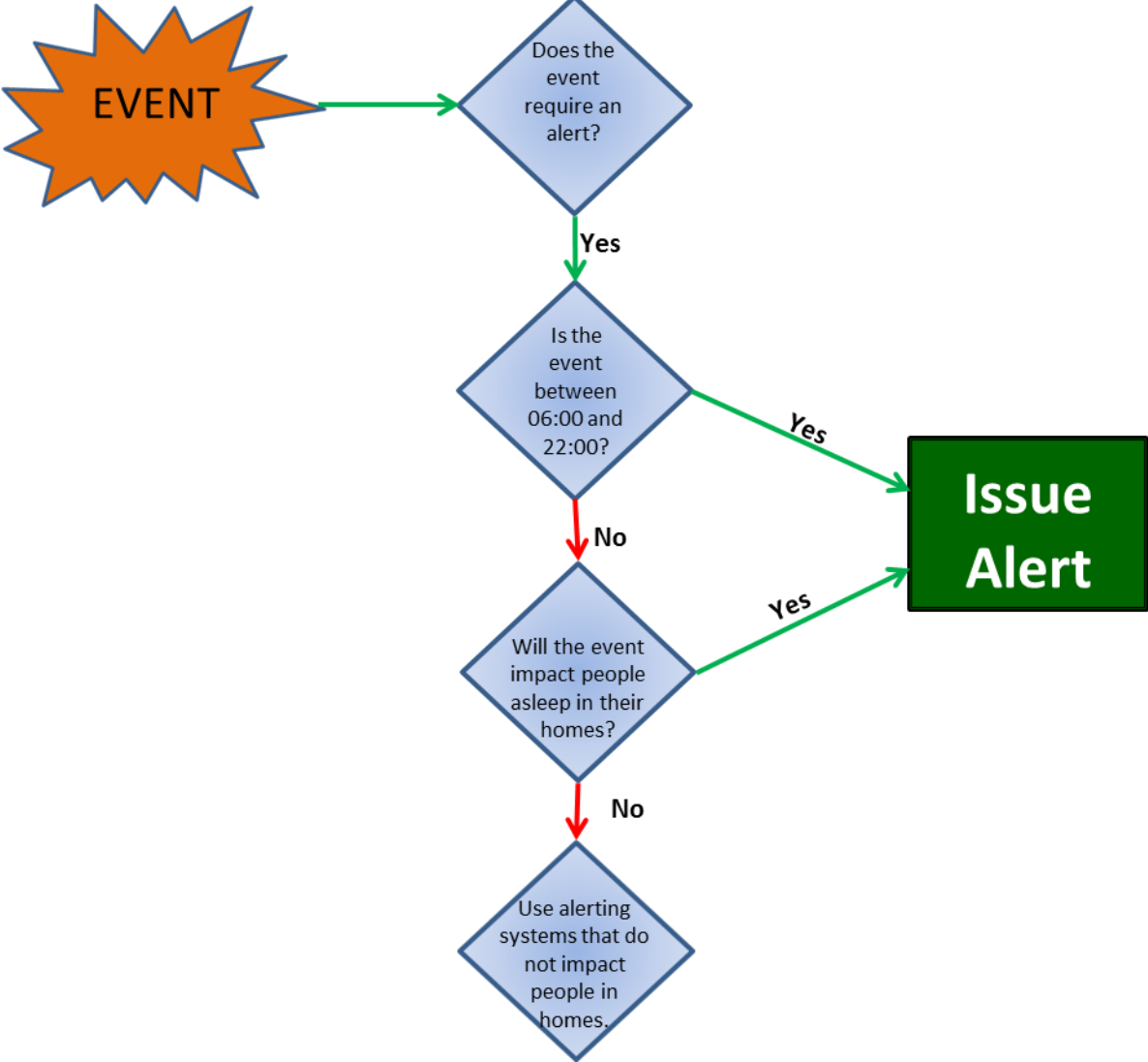
### Scope:
This guideline applies to staff and volunteers of Central County and all subordinate political jurisdictions for the use of Central County public alerting systems.

### Guidelines:
Users must select the appropriate system to use based on the emergency. The following systems will affect people in their homes at night and should only be used for emergencies that have an impact on the public in their homes:

- IPAWS – WEA
- ENS
- Radio alerting systems

The following guidelines can be used:

**EVENT**

Does the event require an alert?

**Yes**

Is the event between 06:00 and 22:00?

**Yes** → Issue Alert

**No**

Will the event impact people asleep in their homes?

**Yes** → Issue Alert

**No**

Use alerting systems that do not impact people in homes.

**LOGO**

# Central County
## Standardized Operational Guidelines

Number: **104**

Subject: **Alerting Process Guidelines**      Effective Date: **01-01-2013**

Approved By: _____      Version #: **2**      Version Date: **01-01-2014**

**Purpose:**
Alerting process guidelines describe the processes used to initiate alerts to the public. Systems have different steps that need to be performed that a user might not remember in an emergency.

**Scope:**
This guideline applies to staff and volunteers of Central County and all subordinate political jurisdictions for the use of Central County public alerting systems.

**Guidelines:**
After the message and the target audience have been determined, users will activate the appropriate systems.

Sirens
- On the siren panel, turn key to "on"
- Select appropriate button to activate
- Activate sirens
- Review log to ensure sirens sounded
- Log activation

IPAWS
- Open the xxx application on the supervisor's computer
- Enter user name and password
- Select pre-formatted template and make needed edits or enter new message
- Select appropriate dissemination channels
- Enter remaining needed information
- Review completed message
- Send message
- Log activation

For any CSEPP community emergency, the alert will be re-sent according to alert and notification plans. For all other emergencies, the need to re-send an alert should be reviewed after 30 minutes or less depending on the emergency.

**LOGO**

# Central County
## Standardized Operational Guidelines

**Number: 105**

Subject: **Alerting Notification Guidelines**                    Effective Date: **01-01-2013**

Approved By: _____    Version #: **2**        Version Date: **01-01-2014**

**Purpose:**
Alerting notification guidelines describe activities of users after an alert is sent. The alert may have an impact on other agencies, and the alerting authorities should be made aware of the emergency.

**Scope:**
This guideline applies to staff and volunteers of Central County and all subordinate political jurisdictions for the use of Central County public alerting systems.

**Guidelines:**
After any alert or notification is sent to the public using any Central County system, a notification that the message was sent to the public will be sent to the following:
- County Judge
- Emergency Management Director
- 9-1-1 Director
- State EOC

In addition, the nature of the event may require notification of other agencies. When an alert is sent, consider notifying the following if needed:
- Public Information Officer
- Neighboring jurisdictions
- Nearby first responders
- Nearby schools, hospitals, and care facilities
- Nearby mass gatherings
- Roads and highway department

### Purpose:
Guidelines for the use of IPAWS and distribution media for alerting the public to events that may pose a risk to the public due to pre-planned events are vital.

The use of IPAWS during a pre-planned event may be a viable method for alerting the public of the event and mitigating panic and risk to the public and participants. These messages would advise the public of the event and that there is no cause for alarm or warn the public of any risks. This guideline does not supplant the authority of the individual jurisdiction's elected officials and emergency management staff. Any alert must still be approved by the alerting authority for the jurisdiction before being sent.

### Scope:
This guideline applies to staff and volunteers of Central County and all subordinate political jurisdictions for the use of Central County public alerting systems.

### Guidelines:
During the planning of a pre-planned event (exercise or public event), the risks associated with the event should be identified. If the planned event has a potential risk to the public or public safety, the use of IPAWS to mitigate that risk may be appropriate. During the planning for each event, the authority will review the event and identify risks. These risks are reviewed against permitted uses and target audiences of the various IPAWS dissemination media. The alerting authority will determine if the use of IPAWS is appropriate. Guidelines for the use of IPAWS should be defined and documented in the event plan or an appendix.

For an alert to be sent to the WEA system, the event must meet the following criteria in accordance with 47 CFR 10.400:

> *(1) Urgency. The CAP Urgency element must be either Immediate (i.e., responsive action should be taken immediately) or Expected (i.e., responsive action should be taken soon, within the next hour).*

*(2) Severity. The CAP Severity element must be either Extreme (i.e., an extraordinary threat to life or property) or Severe (i.e., a significant threat to life or property).*

*(3) Certainty. The CAP Certainty element must be either Observed (i.e., determined to have occurred or to be ongoing) or Likely (i.e., has a probability of greater than 50 percent).*

**Message Format/Content:**
When using IPAWS for a pre-planned event, the alerting authority has the ability to write alert messages in advance to properly communicate the message. Using message templates, various expected messages should be developed to use or have available in the event they are needed.

The alerting authority must be identified in all alert messages.

Each audience, message and distribution media should be reviewed. Is the audience smaller than the distribution media will reach? Will the message cause more concern to the public than the event? Below are some general guidelines for using the available distribution media.

It is not recommended that the authority use WEA messages unless it has the ability to include and edit the free-form 90 character <CMAMText> element into the CAP message.

The WEA message will also allow the alerting authority to make effective use of the <expires> element to keep alerts active for the time of the event. WEA messages, unlike EAS, will be broadcast to phones as they enter the selected area of the alert until the <expire> time.

EAS alerts will be distributed to the broadcast audience, which is often larger than the intended audience. For an event that is small and limited to a specific area, EAS may not be the best distribution medium. Understanding how your local broadcast stations are configured is important in selecting the proper distribution media.

NWEM is also sent to a transmitter that has a large coverage area. Users can use Specific Area Message Encoding (SAME) technology to limit this area, but this will still alert an entire county. In some cases, local broadcast media will monitor the NWEM feed and rebroadcast alerts as an EAS message.

When determining the event code to use, the following definitions of some common codes from the NWS Instruction 10-518 *Non-weather Related Emergency Products Specifications* are provided to assist in compiling the alert message.

> ***Civil Danger Warning (CDW).*** *A warning of an event that presents a danger to a significant civilian population. The CDW, which usually warns of a specific hazard and gives specific protective action, has a higher priority than the Local Area Emergency (LAE). Examples include contaminated water supply and imminent or imminent or in-progress military or terrorist attack. Public protective actions could include evacuation,*

*shelter in place, or other actions (such as boiling contaminated water or seeking medical treatment).*

***Civil Emergency Message (CEM).** An emergency message regarding an in-progress or imminent significant threat(s) to public safety and/or property. The CEM is a higher priority message than the Local Area Emergency (LAE), but the hazard is less specific than the Civil Danger Warning (CDW).*

***Local Area Emergency (LAE).** An emergency message that defines an event that, by itself, does not pose a significant threat to public safety and/or property. However, the event could escalate, contribute to other more serious events, or disrupt critical public safety services. Instructions, other than public protective actions, may be provided by authorized officials. Examples include a disruption in water, electric or natural gas service, or a potential terrorist threat where the public is asked to remain alert.*

***Law Enforcement Warning (LEW).** A warning of a bomb explosion, riot, or other criminal event (e.g. a jailbreak). An authorized law enforcement agency may blockade roads, waterways, or facilities, evacuate or deny access to affected areas, and arrest violators or suspicious persons.*[19]

**Procedure:**
When using IPAWS for a pre-planned event, the following procedures should be followed:

1. Determine the need
   - Determine the event and expected outcomes
   - Determine the risks involved
   - Determine the benefit that IPAWS can bring to mitigating these risks

2. Determine whether the use of IPAWS is a benefit and is permitted
   - Alert authority determines that the use is appropriate given the risk and benefits
   - Incorporate IPAWS into planning process
   - Develop message templates

3. Coordinate with other jurisdictions and public and private partners
   - Notify surrounding jurisdictions of the plan
   - Notify the State of the plan

4. Execute the plan
   - Follow the plan for the use of IPAWS

---

[19] National Weather Service, Operations and Services; Public Weather Services, NWSPD 10-5, *Non-Weather Related Emergency Products Specification* (Instruction 10-518, July 28, 2010)

- Notify surrounding jurisdictions when it is activated
- Notify the State when it is activated
- Notify all parties of any changes in the plan
- Notify all parties when event is completed

## Appendix I – Model Public Affairs Communications Plan

The Public Affairs Communications Plan can be found on the following pages and as an attached Word file.

*The remainder of this page intentionally left blank.*

# Public Affairs Communications Plan

# Integrated Public Alert and Warning System (IPAWS) Test

"*A public that can and will protect itself in the event of a chemical emergency*"
—Public Affairs IPT Mission Statement

The primary purpose of this plan is to mitigate public and media concerns that could arise because of the test of the Integrated Public Alert and Warning System (IPAWS) including Wireless Emergency Alerts (WEA). This plan outlines the methods that will be used to provide coordinated, consistent messages while ensuring that all parties (internal and external) are aware of the test and are provided the opportunity to become familiar with the new means of public alert and warning.

## ACTION PLAN

**Key Audiences:**

- Primary: External—people who live or work in the CSEPP response zones (Immediate Response Zone [IRZ] and Protective Action Zone [PAZ])
- Secondary: Internal—staff, partner agencies, and key community communicators

**Key Messages:**

- New way to warn the public in emergencies.
- Testing following the CSEPP Exercise on Month Day, Year
- Here's what the public will see or hear:
    - EAS message
    - Text Message on cell phone.
- Here's how to get more information_____.

**Designated Spokespersons:**

- Major County: John Doe, Public Information Officer, (555) 555-2345
- State: Jane Doe, Public Information Officer, (555) 555-1234
- Other PIOs?

**Activities:**

| Date | Activity | Responsibility | Date Accomplished |
|---|---|---|---|
| | **Development of key messages and designated spokespersons.**<br>A common set of talking points allows all players to emphasize basic points while referring more technical questions to the appropriate designated spokesperson(s). | John/Jane | 7/18/2013 |
| | **Distribution / integration of key messages and tools.**<br>Provide the public affairs team and other appropriate internal team members the key messages and designated points of contacts. | John | |
| Ongoing | **Respond to / document media or public inquiry.**<br>Use key messages to respond to media or public inquiry. Keep fellow site public affairs officers appraised of media contacts and questions. Document contact in case follow-up is needed at a later date. | PIOs | Ongoing |
| | **Modify existing outreach tools to reflect new IPAWS alerts.**<br>Tabletop display, PowerPoint presentations, website pages | Websites—<br><br>PowerPoint presentations—Public Information Officers (PIOs) modify their power points with new slides. | Web—October 20<br><br>PowerPoint presentations—October 20 |
| | **Key message integration into CSEPP presentations, outreach events, tours, briefings.** | PIOs | October 20 |
| | **Key message integration into Depot presentations, outreach events, tours.**<br>CSEPP will provide talking points for Depot Public Assistance Officers (PAOs) and Outreach Office personnel to use in their presentations, at outreach events, and during tours. | John | October 20 |
| City Councils<br><br><br>CAC | **Elected official/legislative briefings.**<br>Presentations relating to CSEPP activities are given on an ongoing basis to local emergency management boards, first responders, elected officials, legislative aides, and the Citizens' Advisory Commission (CAC). Updates will be given in person, by fax and email, and by telephone. | City Councils—<br><br><br>CAC— | City Councils—<br><br><br>CAC—September 10 |

| Date | Activity | Responsibility | Date Accomplished |
|---|---|---|---|
| Production<br>Ready for demo by October 1<br><br>Ads run<br>Radio—all October?<br><br>TV—Nov. 11–15<br><br>Print—Nov 10–17 | **Paid advertisements.**<br>Incorporate key messages into paid advertisements in newspapers and on radio. | Radio—<br><br>Print—<br><br>TV— | November XX—production complete |
| Chamber of Commerce Deadlines<br>Oct. XX, Mycity<br>Oct. XX, Anytown<br>Nov. XX, ???<br><br>City<br>Oct. XX, Mycity<br>Nov. XX, Anytown<br>Nov. XX, ???<br><br>Business<br>Hospitals | **Newsletter / Public (outreach).**<br>CSEPP will target the August editions of area civic and business newsletters for placement of a story about the IPAWS test. | Research deadlines and how to submit—<br><br>Distribution of article— | October XX—e-mailed |
| September XX<br><br>?? TBD<br>Detonator | **Newsletter / employee and partner agency (in-reach).**<br>CSEPP will provide an article on the IPAWS test for two newsletters: the "News," which is produced on a monthly basis, and the "Detonator," which is produced on a ??? basis. Both are distributed to employees and partner agencies with the idea that they are program representatives in the eyes of their families, friends, and neighbors. | | |
| | **Social Media**<br>Update social media pages and put out messages notifying the public. | Facebook—<br>• Prepare Website—<br>• County—<br>• State— | |

| Date | Activity | Responsibility | Date Accomplished |
|------|----------|----------------|-------------------|
| November 5<br>November 12<br>November 19 | **Personal notifications.**<br>A series of three emails will be sent CSEPP staff, partner agencies, responders, and key community communicators (i.e., police and fire chiefs, elected officials, school districts and CAC members) to advise them of the change and provide answers they can use if questioned. | | |
| | **Press release.**<br>Press release on IPAWS test will be prepared and sent to local newspapers and broadcast media. | John | <mark>October/November XX—media campaign release</mark> |
| | **Live appearances on local broadcast media (radio and TV) programs.**<br>Schedule live appearances on local radio and/or cable TV talk shows. | Schedule—<br><br>Appear— | <mark>November XX—local radio interview</mark><br><mark>November XX—local radio interview</mark> |
| October 23<br><br>November 13 | **Messaging to Broadcasters.**<br>Chair Broadcasters Association will send an ECAST message to state broadcasters but needs to be reminded.<br>Month prior: send reminder that Automatic relay for Civil Emergency messages need to be configured<br>Week prior: send reminder that the test will be taking place. | | |
| | **Highway Reader board.**<br>Ensure that the reader board has information that there is a text-message exercise in progress. | | |
| December | **Annual Report.**<br>The IPAWS test will be noted in the end-of-the-year CSEPP report. | | |

**Performance Measurement:**

The Public Affairs team will attempt to assess the impacts and success of this plan by monitoring both outputs (activity generated because of these actions) and outcomes (public knowledge).

Outputs: Statistical information will be gathered in the following areas:
- Media inquiries
- Media stories generated
- Public phone calls
- Number of web page hits
- Response pieces mailed
- Presentation requests

Outcomes: Public knowledge, changes in knowledge, and/or knowledge voids can be assessed in part using ongoing public surveys being conducted in partnership with the site and Public Affairs team. Surveys conducted prior to the implementation of this plan will serve as a baseline for prior knowledge.

# Appendix J – Model Message Template and Example

The Message Template and an example can be found on the following pages and as an attached Word file.

*The remainder of this page intentionally left blank.*

# EMERGENCY ALERT MESSAGE

## Agency / Jurisdiction Name
Address
City, State XXXXX
Phone: (XXX) XXX-XXXX

Insert Agency
Logo Here

| Date: | Time: | Event Code: |
|---|---|---|
| | | *(Required 3 character code)* |

**Headline**
*160 characters or less including spaces.*

**Insert text here**

**Description:** *What, where, how does this impact the public, for how long?*
*Description and Instruction combined must be less than 160 words.*

Insert text here.

#[incident name]

**Instruction:** *What to do to stay safe and how to do it.*
*Description and Instruction combined must be less than 160 words.*

Insert text here.

**WEA Message (Parameter CMAMtext)**
*This is the message that will be received on cell phones.*
*90 characters or less including spaces. Cannot contain URL or phone number links.*
*It must include sending agency identifier, e.g., NWS or Sheriff.*

Insert text here.

**Twitter Message**
*140 characters or less including spaces.*

Insert text here. #[incident name]

Hint: To find the word and/or character count, highlight the text and click "Words:" in the bottom left of your screen. The pop-up box will show the word and character count (with spaces.)

# EMERGENCY ALERT MESSAGE <mark>[SAMPLE]</mark>

## Best County Emergency Management Agency
123 South Main Street
Anytown, Kentucky 54321
Phone: (555) 555-1234  Fax: (555) 555-5678

| Date: February 28, 2014 | Time: 10:05 a.m. | Event Code: SPW |
|---|---|---|

### Headline
*160 <u>characters</u> or less including spaces.*

## County shelter-in-place advised due to Army Depot emergency

### Description: *What, where, how does this impact the public, for how long?*
*Description and Instruction combined must be less than 160 <u>words</u>.*

At 10:00 AM today, an incident occurred at the Army Depot near Anytown that involved the release of toxic chemicals in areas of Best County. Due to the expected health effects of these chemicals, emergency officials are recommending immediate shelter-in-place for people in the following zones: 1-A, 1-B.

Zones 1-A and 1-B include the following communities: Anytown, Mycity, and Best.

Other areas in Best County are not affected at this time, but residents should stand by for additional information. #Release01

### Instruction: *What to do to stay safe and how to do it.*
*Description and Instruction combined must be less than 160 <u>words</u>.*

To shelter-in-place, do the following:
- Move inside immediately
- Close and lock all windows and doors
- Turn off ventilation system and all fans
- Go into and seal your chosen room with plastic sheeting and duct tape
- Listen to local radio stations via portable battery operated radio

Stay tuned to this station for updates and instructions for Best County residents.

### WEA Message (Parameter CMAMtext)
*This is the message that will be received on cell phones.*
*90 <u>characters</u> or less including spaces. Cannot contain URL or phone number links.*
*It must include sending agency identifier, e.g., NWS or Sheriff.*

BC EMA: Chemical Depot emergency. Shelter-in-Place now. CSEPP Zones 1-A & 1-B.

### Twitter Message
*140 <u>characters</u> or less including spaces.*

Immediate Shelter-in-Place in CSEPP Zones 1-A and 1-B advised to due to chemical emergency at Grass Depot. #Release1

*This page intentionally left blank.*