

# **Minnesota**

## **Public Alerting Authorities**

### **Best Practice Guide**

---

**Statewide Emergency Communications Board, Integrated Public Alert and  
Warning System (IPAWS) Committee**

Approved by the Statewide Emergency Communications Board

**November 2015**

This document describes the recommended best practices, standards, and contact information to assist local jurisdictions with writing templates and managing their mass notification systems in regards to usage with the Integrated Public Alert and Warning System.

# Table of Contents

DOCUMENT REVISION HISTORY.....	iii
Section 1: Alerting Best Practices .....	1
Overview .....	1
Optimum Use of Alerting Systems.....	1
Coverage Differences of Alerting Systems.....	1
Emergency Alert System (EAS).....	1
Wireless Emergency Alert (WEA).....	2
NOAA WEATHER RADIO (NWS) – Non-Weather Emergency Messages (NWEM) .....	5
Outdoor Warning Sirens .....	7
Electronic Telephone Notification Systems .....	7
Social Media .....	7
Alert Codes Authorized by the SECB to Local Authorities .....	7
Civil Danger Warning (CDW) .....	7
Evacuation Immediate (EVI).....	8
Shelter in Place Warning (SPW) .....	8
Civil Emergency Message (CEM).....	8
Required Weekly Test (RWT) .....	8
Alert Codes Authorized to State Authorities .....	9
Nuclear Power Plant Warning (NUW).....	9
Child Abduction Emergency (CAE) .....	9
Required Monthly Test (RMT).....	9
Criteria for Issuing Warnings.....	11
Characteristics of Effective Alert Messages .....	12
Composition .....	12
Style of Writing .....	13
Access and Functional Needs.....	13
English as a Second Language.....	13
Advantages of Templates for Standardizing Messages .....	14
Prevent Errors .....	14

Reduce Delays .....	14
Multilingual Option .....	14
Reduce Coordination Time .....	14
WEA Message Templates.....	14
General Guidelines.....	14
Assign Values.....	15
Emergency Alert System (EAS) Message Templates.....	18
EAS Messages.....	18
Technical considerations for writing an EAS template: .....	18
EAS Message Example.....	19
Response Type .....	19
Headline .....	19
Description Text .....	19
Instruction Text.....	20
Note: If a web site is used ensure it will be able to handle the demand of the potential traffic it may see during an emergency.....	20
Consequences of Unclear, Incorrect, and False-Alarm Messages .....	20
Tips for Text To Speech Messaging.....	21
Agency Coordination.....	23
Bordering Alerting Authorities.....	23
Specialized Communities .....	23
Private Sector Alert Disseminators - Broadcasters .....	23
Private Sector Alert Disseminators - Cell Carriers.....	23
Testing.....	24
Interagency testing .....	24
Coordination .....	24
Consistency .....	24
Resources .....	25
Section 2: Collaborative Operating Groups .....	26
Section Overview .....	26
Definition .....	26
COG Setup Permissions.....	26

Best Practices for COG Management .....	28
Delegating Alerting Authority .....	28
Changing COG Permissions .....	29
IPAWS-OPEN Access.....	29
Identification of the Originator.....	30
Resources.....	32
Points of Contact:.....	32
Wireless Emergency Alert Worksheet .....	33
Testing with the IPAWS Lab at the Joint Interoperability Test Command (JITC).....	35
Notes:.....	36

This guide is designed to serve as both as training and a resource document. The Minnesota Public Alert and Warning System Best Practice Guide is a living document, and suggested changes may be submitted to the IPAWS Committee for consideration.

This guide does not provide vendor specific guidance on operation of software systems.

## DOCUMENT REVISION HISTORY

Date	Revision	Notes	Name
11-2-2015	Initial release		John Dooley
1-15-2016	1.1	Fixed IPAWS Email address and deleted contact	John Dooley

# Section 1: Alerting Best Practices

## Overview

This section introduces you to the skills required to send appropriate, effective, and accessible warning messages using best practices in alerting. Including how to:

- Coverage area issues
- Authorized non-weather alert codes
- Alerting options
- Criteria for issuing warnings
- Identifying the characteristics of effective alert messages
- Writing templates that can be used for effective alert messaging
- Writing effective alert messages
- Identifying system capabilities and limitations with text to speech (TTS)
- Identifying best practices for agency coordination and public education for alerts and warning

## Optimum Use of Alerting Systems

### Coverage Differences of Alerting Systems

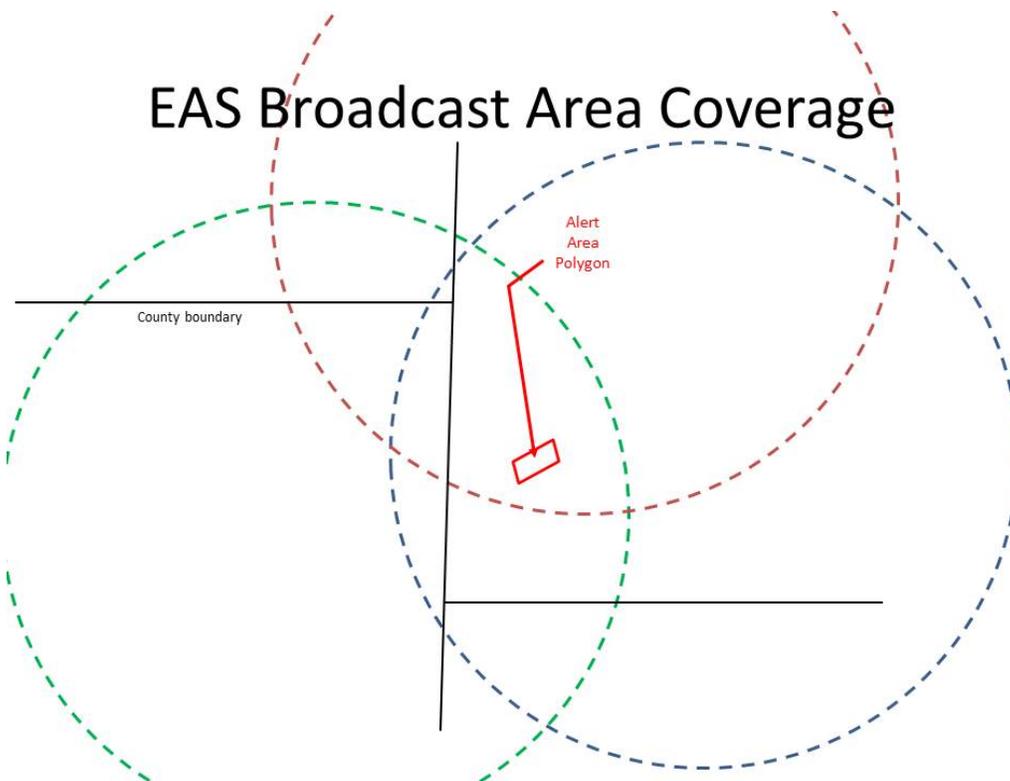
When preparing to send out alert messages, it is important to understand the potential coverage area provided by each alerting system. The following guidance shows how to incorporate each system into a layered approach starting from the system with the broadest reach to those that are capable of being scaled down to a small geographically targeted area.

### Emergency Alert System (EAS)

EAS covers the broadest area of all the alert systems. When a local agency sends an alert for its county, it will overlap with other counties depending on how each EAS participant has their equipment programmed. When an alert is sent, be advised it will cover a very large area beyond the jurisdiction that sent the alert. EAS participants are encouraged by the Minnesota state EAS plan to configure the decoder equipment to receive, decode and broadcast the authorized alert codes published in the plan. Jurisdictions are encouraged to work with local EAS participants to confirm that equipment is properly programmed and confirm that the EAS participant's policy is included in the jurisdiction's planning process.

In the diagram on the next page, the larger dotted line circles show potential broadcast EAS participant area coverage as compared to the alert area polygon.

## EAS Broadcast Area Coverage



### Wireless Emergency Alert (WEA)

Wireless Emergency Alerts are received on most new cell phones<sup>1</sup>. The unique ring tone and vibration is designed to get the public's attention and alert them to an imminent threat. The WEA system is designed to be an “OPT OUT” system. Phones are shipped from the factory with all of the three alert categories turned on Presidential, Imminent Threat and AMBER. The user can turn off the Imminent Threat and AMBER alerts but cannot turn off the Presidential alert.

Wireless Emergency Alerts are broadcast to the user through the carrier’s control channel and are not susceptible to network congestion like normal SMS (Short Messaging Service) text messages or voice calls. As an “OPT OUT” system the persons in the alert area do not have to be subscribed to the local system; WEA alerts users based on their location.

It is recommended that WEAs be used for localized incidents. Once a WEA is sent out, it may be followed up with an EAS message that provides more details if the situation escalates to a larger coverage area and expands the alert area.

WEAs can work hand-in-hand with other alerting systems to create a more layered approach; if one system does not get the public’s attention, another alerting systems redundancy may increase the likelihood the message reaches the public.

---

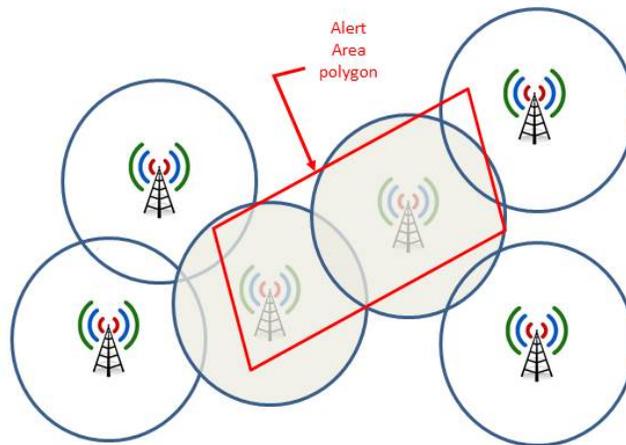
<sup>1</sup> Cellular telephones manufactured since January of 2012 have to be WEA capable by FCC ruling.

The coverage area of a WEA depends on the location of the cell towers in the affected area. With WEAs, the geo-targeted area can be small. Alert originators need to be aware of the cellular coverage and deployment technology. If possible the jurisdiction should contact the carriers that service their area to verify what implementation variation they are using. If the designated alert area polygon is compared with the affected area to which the message should be sent, it can be determined whether there will be message “overreach” or “under reach”. Both WEA and EAS may need to be used.

## WEA Carrier Implementation: Variation 1

- Alert is broadcast only from towers **located inside alert area** polygon defined in the IPAWS message.

Note: Phones located between towers inside and outside the Alert Area may be connected to a tower not broadcasting the WEA.

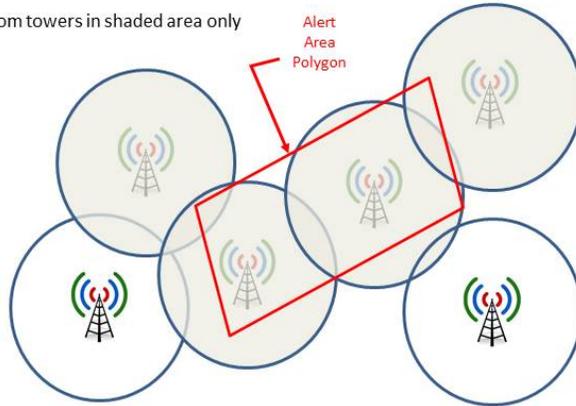


A - WEA Carrier Implementation: Variation 1

## WEA Carrier Implementation: Variation 2

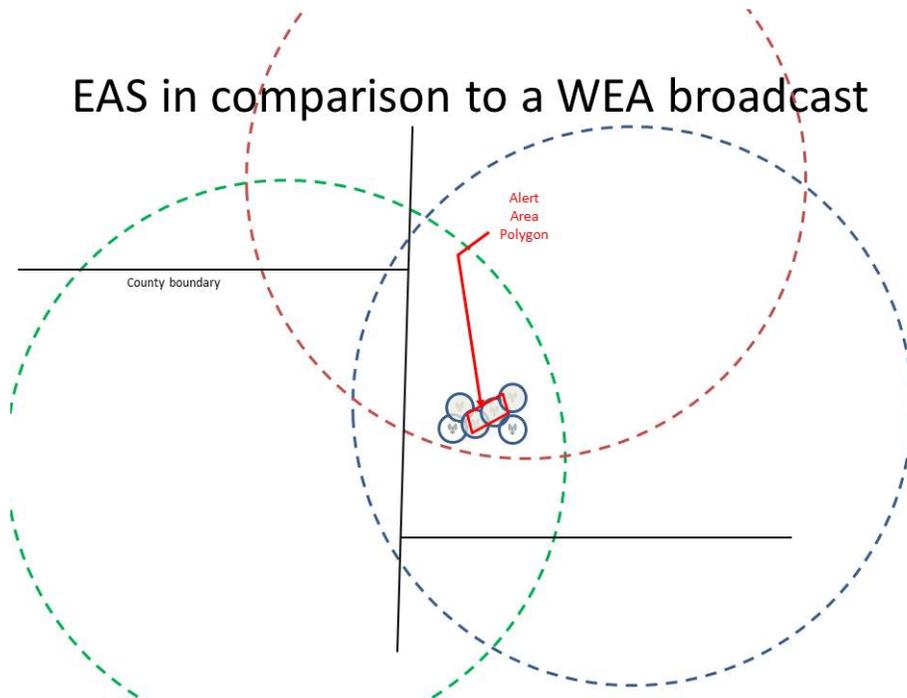
- Alert is broadcast from towers with estimated coverage that includes a part of the alert area polygon defined in the IPAWS message.

WEA is broadcast from towers in shaded area only



B - WEA Carrier Implementation: Variation 2

### WEA coverage compared to EAS



## **NOAA WEATHER RADIO (NWS) – Non-Weather Emergency Messages (NWEM)**

NOAA (National Oceanic and Atmospheric Administration) Weather Radio All Hazards (NWR) is a nationwide network of radio stations broadcasting continuous weather information directly from the nearest National Weather Service office. NWR broadcasts official Weather Service warnings, watches, forecasts and other hazard information 24 hours a day, 7 days a week.

Known as the "Voice of NOAA's National Weather Service," NWR is provided as a public service by the NOAA, part of the Department of Commerce. NWR in Minnesota includes approximately 48 transmitters covering the state and adjacent coastal waters (Lake Superior). NWR requires a special radio receiver or scanner capable of picking up the signal. Broadcasts are found in the VHF public service band at these seven frequencies (MHz):

162.400	162.425	162.450	162.475	162.500	162.525	162.550
---------	---------	---------	---------	---------	---------	---------

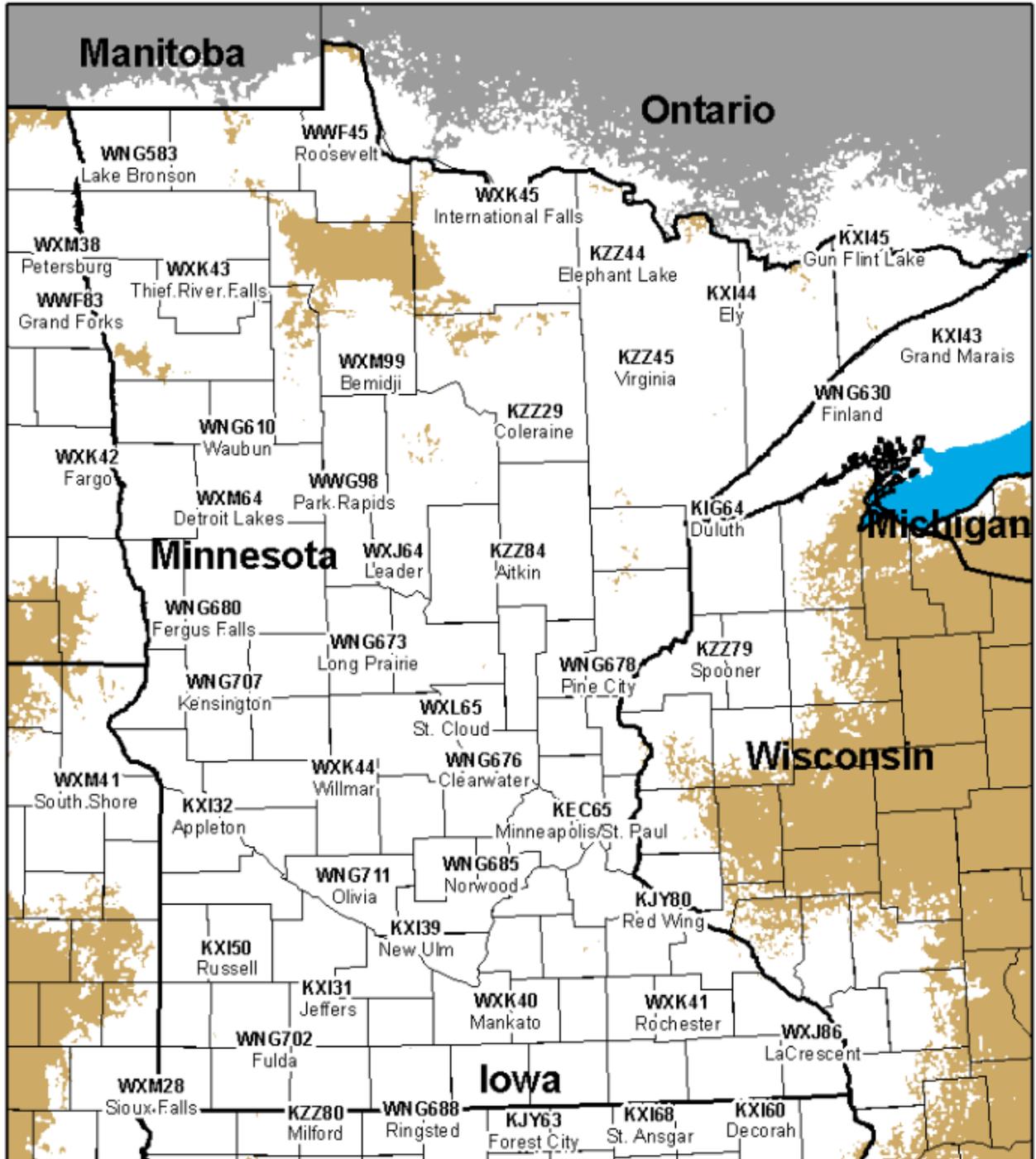
- Currently the NWS has connectivity with FEMA IPAWS. NWS is the only agency authorized to send a weather related alert
- The only way for public safety officials to use the NWS NWEM system is to have a Memorandum of Agreement between the jurisdiction and the servicing National Weather Forecasting office with a procedure in place to send a NWEM to the servicing NWS office for broadcast through the NWR system.
- As of the publishing date of this best practice guide there are no authorized Minnesota COGs that can send an alert through the FEMA IPAWS OPEN system to the NWS system.

Most EAS participants monitor the NWR frequency that covers their broadcast area and may retransmit these warnings to their audience.

Citizens who have a NWR radio in their house or workplace must program the radio to receive the specific alerts.

The most current NWR transmitter map can be found at:

<http://www.nws.noaa.gov/nwr/Maps/PHP/MN.php> which shows the status of the transmitters.



## **Outdoor Warning Sirens**

Outdoor warning sirens have been in place for decades to warn the public that there is a threat to their safety outdoors. Local policy dictates the activation and use of this system.

## **Electronic Telephone Notification Systems**

Electronic Telephone Notifications Systems are also referred to as “OPT IN” systems into which local jurisdictions imports wire line telephone directory data and get the public to enroll to receive community information or alert notifications via wireless phones or email. The challenge for public safety is the public seems reluctant to sign up for alerts, despite strong efforts to get them onboard. There are two approaches to address this challenge:

- Launch an effective outreach campaign.
- Accept that even a strong campaign will still leave enrollment gaps and plan to work around the gaps by developing a layered warning approach of using multiple systems at once.

## **Social Media**

Social media is too powerful a means not to be recognized as an alerting tool. Persons who want to know what is going on in their community often use this as a means to be informed. Just as with the Electronic Telephone Notification system jurisdictions need to have the public “follow” them on these mediums (i.e. Facebook, Twitter and more). Social media needs to stay current or users will stop following posts. If they have stopped following the jurisdiction’s social media, messages will not be received.

## **Alert Codes Authorized by the SECB to Local Authorities**

### **Civil Danger Warning (CDW)**

A CDW is a warning of an event that presents a danger to a significant amount of the local civilian population. The CDW usually warns of a specific hazard and gives specific protective action. Examples include contaminated water supply, imminent or in-progress military or terrorist attack. Public protective actions could include evacuation, shelter in place, avoid the area, or boiling contaminated water.

- Can be used as a Wireless Emergency Alert (WEA) and or an Emergency Alert System (EAS) warning message.
- Use it to cover a large area.

## **Evacuation Immediate (EVI)**

An EVI warning is where an immediate evacuation is recommended. For example, in the event a flammable or explosive gas is released, authorized officials may recommend evacuation of designated areas where casualties or property damage from a vapor cloud explosion or fire may occur.

- Can be used as a Wireless Emergency Alert (WEA) and could also be an Emergency Alert System (EAS) warning message.

## **Shelter in Place Warning (SPW)**

A warning of an event where the public is recommended to shelter in place (go inside, close doors and windows, turn off air conditioning or heating systems, and turn on the radio or TV for more information) or to take cover from a dangerous situation in their area (This will need to be defined in your message to them). An example is the release of hazardous materials where toxic fumes or radioactivity may affect designated areas.

- Can be used as a Wireless Emergency Alert (WEA) and/or an Emergency Alert System (EAS) warning message.

## **Civil Emergency Message (CEM)**

The CEM is 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 a news release, but the hazard is less serious or smaller in scope than a Civil Danger Warning (CDW). For example, the CEM could be used to warn a small concentrated area via the Wireless Emergency Alert System.

- Sent as Wireless Emergency Alert (WEA)
  - According to the state EAS plan the EAS system message should only create a log entry in the EAS participants (i.e. broadcast/cable) equipment. It is not expected to go out over the air, but may be broadcast at the discretion of the EAS participant. This would be a way of informing the media of an emerging event.

## **Required Weekly Test (RWT)**

Weekly testing of local systems ensures they have connectivity to the IPAWS OPEN server and that messages can be sent through the system. The RWT is only logged in the local EAS participants equipment. This test does not go out to the public. This is where relationships with the local radio, television, wire line telephone (if providing television service) or cable franchise are crucial to ensuring that messages will make it to the public when needed.

- Sent only as an Emergency Alert System (EAS) message for test purposes.

- The RWT can also be used as a training tool for personnel to familiarize them with the third party software package used by the organization.

## **Alert Codes Authorized to State Authorities**

### **Nuclear Power Plant Warning (NUW)**

A warning of an event at a nuclear power plant such as a General Emergency as classified by the nuclear power plant. The alert is confined to an area of less than a 10-mile radius around the plant called the Emergency Planning Zone (EPZ). Authorized officials may recommend evacuation or sheltering within the 10 mile EPZ.

- Can be used as a Wireless Emergency Alert (WEA) and or an Emergency Alert System (EAS) warning message.

### **Child Abduction Emergency (CAE) also known as the AMBER Alert**

In the state of Minnesota only the Bureau of Criminal Apprehension is authorized to send out a CAE alert via EAS or WEA. A CAE is an emergency message, based on established criteria, about a missing child believed to be abducted. Local or state law enforcement agencies investigating the abduction will describe the missing child and provide a description of the suspect or vehicle. The alert message will ask the public to notify the requesting agency if they have any information on the whereabouts of the child or suspect.

### **Required Monthly Test (RMT)**

Monthly testing of the EAS system ensures the state has connectivity to the IPAWS OPEN server and the statewide distribution system is working. The RMT is required to be rebroadcast by every local EAS participant whose equipment forwards the message to the public. This test is a coordinated effort of the Minnesota Broadcasters Association, WCCO-AM, Minnesota Public Radio and the Department of Public Safety. Coordination is crucial to ensuring this message is only sent once at the time published on the first Wednesday of each month.

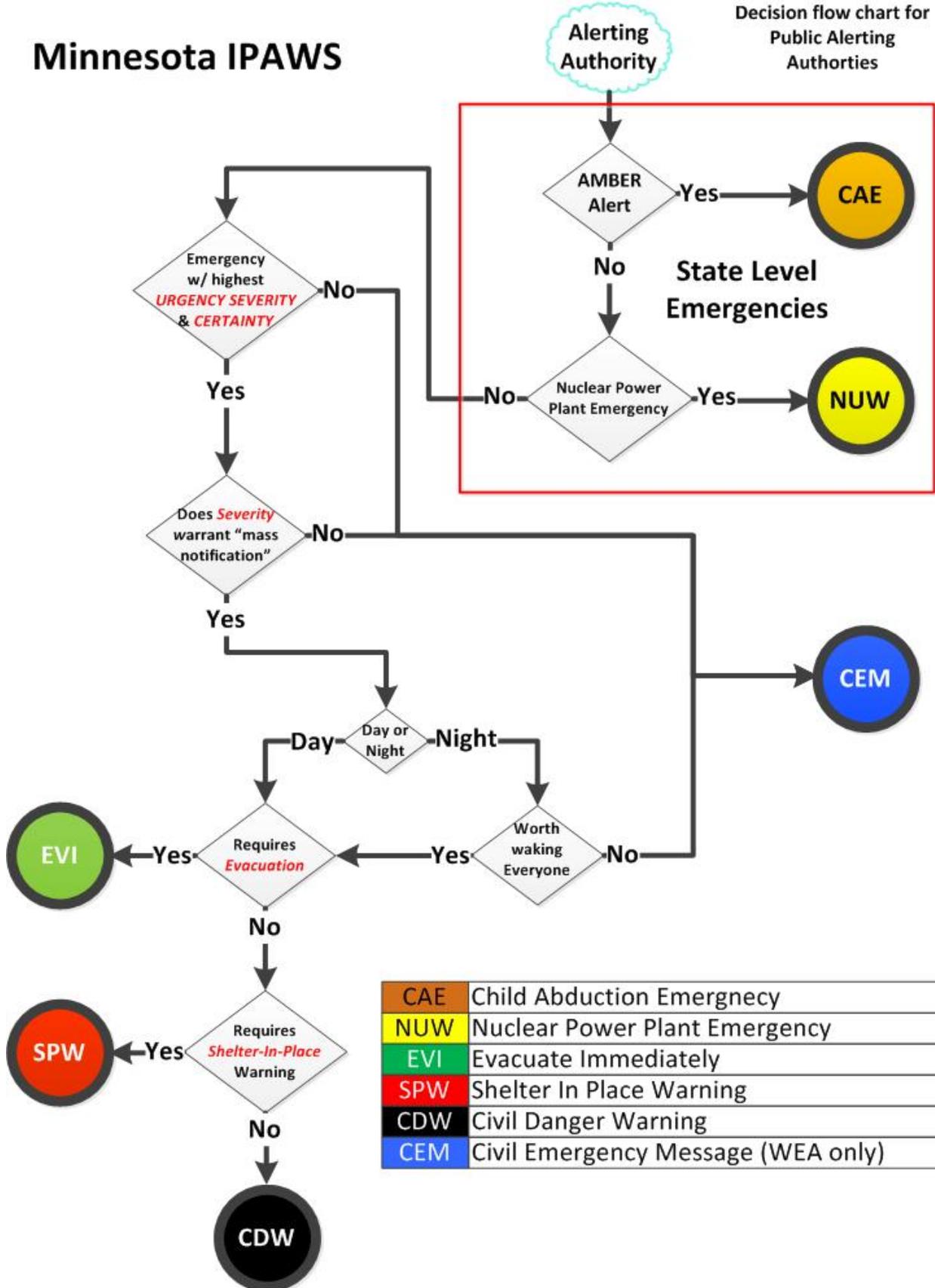
- Sent only as an Emergency Alert System (EAS) message for test purposes.
- Cannot be sent as a WEA test; only federal agencies<sup>2</sup> may conduct these tests via WEA.

---

<sup>2</sup> CFR 47 §10.350 WEA Testing requirements. Subparagraph (4) The RMT shall be initiated only by the Federal Alert Gateway Administrator using a defined test message. Real event codes or alert messages shall not be used for the WEA RMT message.

# Minnesota IPAWS

Decision flow chart for  
Public Alerting  
Authorities



CAE	Child Abduction Emergency
NUW	Nuclear Power Plant Emergency
EVI	Evacuate Immediately
SPW	Shelter In Place Warning
CDW	Civil Danger Warning
CEM	Civil Emergency Message (WEA only)

## Criteria for Issuing Warnings

Deciding whether to issue a public warning can be a difficult decision. Ultimately it will be a matter of local judgment; however, it will be helpful to have an outline of decision criteria to assist with the process and ensure a timely decision is made.

When deciding whether to issue a public warning, the following criteria should 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 that the hazardous situation will occur?
- Are other means of disseminating the information adequate to ensure rapid delivery of urgent information?

## What Code to use

Urgency	Severity	Certainty	= Action Code
Immediate	Extreme	Observed	EVI, SPW, CDW, CEM*
Expected	Severe	Likely	EVI, SPW, CDW, CEM*
Future	Moderate	Possible	Advisory
Past	Minor	Unlikely	Advisory

\* Using a CEM will activate Wireless Emergency Alerts, but not Emergency Alert System

In order to successfully send a Wireless Emergency Alert, the alert must contain certain values for these fields, reflecting "Imminent Threat". The values marked in red are the ones that will trigger a WEA or EAS alert as outlined by the Common Alerting Protocol (CAP) guidelines:

### **(1) Urgency:**

“**Immediate**” - Responsive action should be taken immediately

“**Expected**” - Responsive action should be taken soon (within next hour)

“Future” - Responsive action should be taken in the near future

“Past” - Responsive action is no longer required

“Unknown” - Urgency not known

### **(2) Severity:**

“**Extreme**” - Extraordinary threat to life or property

“**Severe**” - Significant threat to life or property

“Moderate” - Possible threat to life or property

“Minor” – Minimal to no known threat to life or property

“Unknown” - Severity unknown

### **(3) Certainty:**

“**Observed**” – Determined to have occurred or to be ongoing

“**Likely**” - Likely (more than 50% chance)

“Possible” - Possible but not likely (less than 50% chance)

“Unlikely” - Not expected to occur

“Unknown” - Certainty unknown

## **Characteristics of Effective Alert Messages**

### **Composition**

To help ensure that warning messages are effective, they must be issued in a timely manner and should include the following information about the hazard:

- Source – Who is the warning coming from - make it clear.
- Guidance – What do you want the public to do?
- Hazard – What is going to harm them?
- Location – Where is the danger?

- Termination Time – (required by the CAP guidelines)

Source	Guidance	Hazard	Location	Termination Time
--------	----------	--------	----------	------------------

Note: you will see this color coding throughout the examples in this document. They are only intended to highlight the different areas and are not required to be used when making your templates.

## Style of Writing

How you write an alert/warning message is nearly as important as what you write. Some style elements to consider when writing alert and warning messages include:

- Specificity
- Consistency
- Certainty
- Clarity
- Accuracy

## Access and Functional Needs

Effective alert messages also address persons with disabilities and those with access and functional needs. From an access and functional needs perspective, keep the following in mind when composing a message:

- Clear and simple language
- Avoid non-standard language and terminology to facilitate easier text to speech conversion and use of screen reading devices
- Consistency of audio with message text
- Ample text and audio to explain images/maps

## English as a Second Language

The FEMA IPAWSOPEN aggregator does not provide translation services, but it is capable of accepting and relaying alerts in multiple languages as composed by the alert originator. Alert authoring or other software programs may provide automated translation, but all automatically translated text should be validated with a speaker of the language to avoid errors. The use of pre-translated templates may serve to minimize the amount of information requiring translation for actual alerts.

# Advantages of Templates for Standardizing Messages

There are a number of advantages to using templates for standardizing messages.

## Prevent Errors

The use of templates tailored to those hazards likely in a warning area can help prevent errors or omissions that can occur in moments of urgency.

## Reduce Delays

Using a template that incorporates pre-approved language can reduce delays in issuing alerts and warnings.

## Multilingual Option

If multiple languages need to be used, templates can be translated in advance.

## Reduce Coordination Time

Templates prepared in advance can be pre-coordinated with other agencies including the jurisdiction's public information officer (PIO) to reduce coordination effort and time.

# WEA Message Templates

## General Guidelines

When creating templates for WEA messages, you should focus on the required fields.

- Source – Who is the warning coming from - make it clear.
- Guidance – What do you want the public to do?
- Hazard – What is going to harm them?
- Location – Where is the danger?
- Termination Time – (required by the CAP guidelines)

Source	Guidance	Hazard	Location	Termination Time
--------	----------	--------	----------	------------------

Remember in order to successfully send a WEA the alert must contain certain values for the following fields, reflecting "Imminent Threat":

<b>Urgency</b>	<b>Severity</b>	<b>Certainty</b>
<input type="checkbox"/> <b>Immediate</b>	<input type="checkbox"/> <b>Extreme</b>	<input type="checkbox"/> <b>Observed</b>
<input type="checkbox"/> <b>Expected</b>	<input type="checkbox"/> <b>Severe</b>	<input type="checkbox"/> <b>Likely</b>
<input type="checkbox"/> <b>Future</b>	<input type="checkbox"/> <b>Moderate</b>	<input type="checkbox"/> <b>Possible</b>
<input type="checkbox"/> <b>Past</b>	<input type="checkbox"/> <b>Minor</b>	<input type="checkbox"/> <b>Unlikely</b>
<input type="checkbox"/> <b>Unknown</b>	<input type="checkbox"/> <b>Unknown</b>	<input type="checkbox"/> <b>Unknown</b>

Because WEA messages are limited to 90 characters, it is very important to maximize their effectiveness. Consider the following factors when writing WEA messages:

- Does the message drive the recipient to take life-saving action?
- Does it direct people to other sources of information?
- Ensure the message does not contain URLs or phone numbers<sup>3</sup>.

### Assign Values

Messages are required by CAP 1.2 standards to have certain values associated to them to help with standardizing the message formats. The following values and codes are available for selection or sometimes pre-selected by third party alert authoring software depending on the chosen event code.

*Authorized Event Codes* (in Minnesota):

<b>Authorized Code</b>	<b>Code Description</b>
CDW	Civil Danger Warning
CEM	Civil Emergency Message
EVI	Evacuate Immediately Warning
SPW	Shelter in Place Warning
CAE	Child Abduction Emergency (BCA ONLY)
NUW	Nuclear Power Plant Warning (HSEM, BCA and the Chanhasen office of the National Weather Service )

---

<sup>3</sup> CFR 47 §10.440 Embedded reference prohibition. A WEA Alert Message processed by a Participating CMS Provider must not include an embedded Uniform Resource Locator (URL), which is a reference (an address) to a resource on the Internet, or an embedded telephone number. This prohibition does not apply to Presidential Alerts. [78 FR 16808, Mar. 19, 2013]

*Response Type:* (some programs insert this automatically based on the event code)

<b>Response Code</b>	<b>Code Description</b>
Evacuate	Relocate as per instructions
Prepare	Make preparations as per instructions
Execute	Execute a pre-planned activity as per the instructions
Avoid	Avoid the subject event as per the instructions
Monitor	Attend to information sources as per the instructions
Access	Evaluate the information in the message
All Clear	The subject event no longer poses a threat or concern
None	No Action recommended

In some software programs the assigned values may look as follows but they still meet the CAP 1.2 standard (as listed below):

- EVI/Evacuate = "Evacuate Now"
- SPW/Shelter = "Take Shelter Now"
- Prepare = "Prepare for Action"
- Execute = "Execute Action"
- Monitor = "Monitor Radio or TV"
- Avoid = "Avoid Hazard"

Here is an example of a Shelter in Place Warning relayed via WEA.

<b>Field</b>	<b>Example</b>
[Source] Sender Name value, typically associated with the alert originator	Aitkin County Sheriff
[Guidance - What to do] Assigned value derived from instruction-specific event code (EVI, SPW) or response type element	Take Shelter Now
[Hazard - What] Event name corresponding to event code element	Chlorine Gas in air
[Location - Where]	in this area until
Termination Time in local time zone derived from expires element	4:30 PM

A WEA Message would look like this: [# of characters]

<p><b>Chlorine Gas in air this area until 4:30PM Take Shelter Now - Aitkin County Sheriff</b> [85]</p>
<p><b>Aitkin County Sheriff Advises Take Shelter Now - Chlorine Gas in this area until 4:30PM</b> [89]</p>

WEA Category (some programs insert this automatically based off the event code) is part of the CAP 1.2 Standard:

<b>Category</b>	<b>Description</b>
Geo:	Geospatial (including Landslides)
Met:	Meteorological (Including Floods)
Safety:	General Emergency and Public Safety
Security:	Law enforcement, Military, Homeland and Local security
Rescue:	Rescue and Recovery
Fire:	Fire Suppression and Rescue
Health:	Medical and Public Health
Env:	Pollution and other environmental
Transportation:	Public and Private transportation
Infra:	Utility, telecommunication , other non-transport infrastructure
CBRNE:	Chemical, Biological, Radiological, Nuclear and High Yield Explosive
Other Events	

# Emergency Alert System (EAS) Message Templates

## EAS Messages

- EAS messages are free-form messages. They should be coordinated with the PIO in order to ensure they do not conflict with what the PIO is saying.
- The warning message should be written in a style that clearly conveys the potential hazard to the public.
- The content of the message should include information on five basic elements: source of message, description of the hazard/risk, location of the hazard, guidance for protective actions, and time available to act.

### Technical considerations for writing an EAS template:

As stated in the [CAP EAS Implementation Guide](#) the following guidance for constructing alert text for CAP V1.2 IPAWS v1.0 Profile for EAS activations.

- A CAP message contains many free form text elements, many of them optional. The CAP-to-EAS device must pull these various elements together and generate one text string for use in displays, logs, video crawl, and as a source for text to speech generation, if needed by, and supported by the device.
- An 1800 character maximum length is recommended for EAS text. This was chosen based on various requirements, which are primarily the buffer limitations in character generators and other display devices, and the two minute audio time limit imposed by the FCC for EAS messages.

The section below describes a method for constructing the alert display text. Also defined is a single explicit element that will provide the needed text in a single place.

Be aware that text to speech equipment used by EAS participants may automatically make changes. The same changes may be automatically made on alerts intended for use by character generators or other one-line scrolling displays. The CAP/EAS device may collapse the string by one of the following means:

- 1) Removing leading and trailing whitespace.

2) Replacing all whitespace<sup>4</sup> characters with space, and converting runs of spaces to a single space.

### EAS Message Example

The following message was written and highlighted in the related colors to show the five elements were covered. This message has been shortened from the previous example written to be clear and concise.

Source	Guidance	Hazard	Location	Termination Time
--------	----------	--------	----------	------------------

- Remember the recommended 1800 character limit on EAS messages and keep it under the FCC mandated two minute limit for a message.
- In order to have an effective message, key elements should be in the first 20 seconds of the message.

### Example EAS Template

<b>Response Type</b>	Shelter in Place Warning (SPW)
<b>Headline</b>	Description: <b>Aitkin County Sheriff's Office</b> has issued a <b>Shelter in Place warning</b> for <b>southwest Aitkin County</b> <b>until 2:00 am</b>
<b>Description Text</b>	<p><b>The Aitkin County Sheriff's Office</b> has issued a <b>Shelter – In – Place Warning - IMMEDIATELY</b> - at 2:15 pm, an explosion occurred at the <b>Tyson Chemical processing plant</b> in the city of <b>Arlington</b>, in <b>southwest Aitkin county</b>. This explosion has caused a release of chlorine gas which is extremely hazardous to human health if inhaled or comes in contact with human skin.</p> <p>Vapors from this chlorine gas release may not be visible and can cause serious adverse health effects with very little notice. <b>State hazardous materials technicians</b> are closely monitoring the situation. The emergency alert system has been activated to advise people in the immediate area</p>

<sup>4</sup> Whitespace includes the following characters: space, form-feed, new line, carriage return, horizontal tab, and vertical tab.

	<p>surrounding the Tyson Chemical Processing Plant in Arlington. Shelter In Place IMMEDIATELY.</p> <p>Do not attempt to evacuate at this time because you will risk greater exposure by going outside than if you remain indoors. The Shelter In Place zone consists of an area 5 miles around the Tyson Chemical Processing Plant in Arlington. This area is bounded by George Washington High School on the West, Colts Sports Arena on the North, Kilmer Middle School on the East and Ryan Performing Arts Center on the South. If you are within this area, you should Shelter In Place IMMEDIATELY.</p>
<b>Instruction Text</b>	<p>Detailed sheltering instructions have been provided to Arlington area broadcast Radio and Television stations. Please seek out additional information on the county web site <a href="http://WWW.CO.AITKIN.MN.US">WWW.CO.AITKIN.MN.US</a></p>

**Note:** If a web site is used ensure it will be able to handle the demand of the potential traffic it may see during an emergency.

## Consequences of Unclear, Incorrect, and False-Alarm Messages

Unclear or incorrect warning messages may lead to loss of life and property. It is therefore very important to issue accurate and consistent alert messages. The tables on the following pages are provided as guidance for writing text to speech. They show how common mistakes in writing style would be disastrous when trying to send a message using TTS without knowing how systems may respond to written messages. Acronyms and short form words should be avoided whenever possible. When in doubt, spell it out.

## Tips for Text To Speech Messaging

\*\* Note: Acronyms and short form words should be avoided whenever possible. When in doubt, spell it out. \*\*

Category	Correct	Incorrect
Age	42 to 45 years old 42 years old 42 yr old	40-45 42 yrs old
Height	5 feet 6 inches 5 foot 6 165cm, 165 centimeters (or centimeters) 1.2m 1.2 meters	5 ft 6 in 165 cms (cms is not a unit of measure)
Speed	Miles per hour Kilometers per hour km per hour km/h	Mph KmH kms/hr km/hour
Temperature	-30 degrees Fahrenheit +30 degrees Celsius	-30 degrees C (F)
Date	MM/DD/YYYY 02/12/2013 = February 12th, 2013	Only recognizes M-D-Y format.
Time	10:00 AM (PM) 10:00AM (PM)	1800 hours (avoid using the 24 hour clock; recipients may not understand this format.)
Weight	12 lbs ( <i>must have a space</i> ) 12 pounds 13 kg ( <i>plural form does not exist</i> ) Weight	12lbs 12 pds 13kgs wt
Directions	North Northeast East Southeast South Southwest West Northwest	N E S W

Category	Correct	Incorrect
Directions of Travel	Northbound, heading north Southbound, heading south Westbound, heading west Eastbound, heading east	NB (northbound) SB (southbound) WB (westbound) EB (eastbound)
License Plate	A B C 1 2 3 ( <i>must have a space between each character</i> )	ABC123 ABC 123
Non alpha numeric	& % @ #1 (incl number = “number 1”)	_(will be pronounced “underscore”)
Addresses	<ul style="list-style-type: none"> <li>• Ensure proper punctuation and capitalization</li> <li>• 14225 142nd Street</li> <li>• 506 2nd Street N</li> <li>• 100 Ave. to 118 Ave. (requires period with Ave.)</li> <li>• “Suite” needs to be spelled out in full.</li> <li>• Remember that numbers are spoken out in the tens and hundreds. So 12445 = twelve thousand four hundred forty five. <ul style="list-style-type: none"> <li>○ Use spaces between such numbers.</li> </ul> </li> <li>• Be careful about dual use abbreviations. St. = “Saint” rather than “Street”. 506 2nd St. N becomes “Five Hundred and Six, second Saint N”.</li> <li>• Spell out Drive and Highway in full</li> </ul> <p><b>Type out the full text to ensure proper pronunciation</b></p>	
Telephone Numbers	780-980-8758 9 1 1 (spaces need to be included in between each number)	7809808758 780 980 8758 780.980.8758 (780)9808758 911

## **Agency Coordination**

Alert messages that give false alarms or "cry wolf" may cause the public to become frustrated. Alerting Authorities should protect against cry wolf syndrome; too many false alarms may erode public trust, which is a vital element in disaster response. If the issuance of a false alarm is fully explained, the public tends to take into account officials are making difficult decisions to protect them from harm.

Effective alerting demands the presentation of clear and unambiguous information to the public. It is important for communities to partner with each other to aid in effective alerting.

### **Bordering Alerting Authorities**

When multiple alerting agencies possess the ability to issue alerts in an area, confusion can arise from redundant or contradictory alerts. When preparing best practices for alerting, consider cases where an emergency event may cross jurisdictional boundaries, such as a drifting cloud of toxic gas released from an industrial accident, or a flood resulting from a dam break. Establish agreements with adjacent jurisdictions that address coordination of alerting to enable a coordinated and consistent response in advance.

### **Specialized Communities**

Specialized communities in a jurisdiction may be involved with emergencies and the recovery process. These specialized communities will vary greatly in each community and can include, but are not limited to: universities, nuclear power plants, chemical facilities, military bases, federal agencies and hospitals. Some of these entities have the capability to become an IPAWS Non alerting Collaborative Operating Group (COG) to have private messaging access to another authorized alert originator. Public Safety Answering Points (PSAPs) and emergency managers should coordinate with these organizations to better determine the risks that exist in the jurisdiction and how to best coordinate plans in the event of an emergency.

### **Private Sector Alert Disseminators - Broadcasters**

Broadcasters and broadcast engineers are an important part of the alerting process and a strong relationship is critical. The Minnesota EAS plan placed a limit on the types of codes EAS participants are assigned to monitor for EAS broadcast. The Minnesota EAS plan states that some codes are automatically forwarded and some are not. Alerting Authorities need to know which codes are automatically forwarded and which require human intervention to be sent out. This is especially important for stations that are automated and do not have a person at the station during all hours of operation.

### **Private Sector Alert Disseminators - Cell Carriers**

With the addition of WEA's, the involvement of private sector partners in the wireless industry has expanded. Commercial Mobile Service Providers (cellular carriers) partner with FCC and

FEMA to make WEAs a reality. Due to this additional layer of dissemination and the variability of WEA implementation through the carriers, it is critical that Public Safety Answering Points (PSAPs) and emergency managers are aware of which cellular carriers operate in their jurisdictions and what WEA coverage may be available. Four of the major cellular carriers (ATT, Sprint, T Mobile and Verizon) operate in Minnesota; they are all participants in the WEA program. Each PSAP receives data from the carriers on the detailed locations and capabilities of the towers in their jurisdiction. This information could be used as awareness training for personnel involved in alerting as to where to draw their polygon in order to maximize the coverage needed when sending out a WEA.

## **Testing**

It is important to test your templates. Testing methods maybe devised locally with assistance from software vendors during training, or with instructions from the Joint Interoperability Test Command (JITC). JITC maintains the IPAWS functional laboratory and provides FEMA interoperability and functional testing support, Information Assurance (IA) support, and overall technical support. See page 35 for details.

## **Interagency testing**

Collaborative Operating Group to Collaborative Operating Group (COG) testing is another way to ensure that COGs are communicating with their neighboring or partner jurisdictions. This testing can familiarize staff with this feature and save time when neighboring jurisdiction must be notified of an emerging hazard or event which may be headed their way.

## **Coordination**

When possible communication of WEA message will be released to the media before the alert goes out, to address the "check your local media" action. This coordination will ensure that the broadcast community and local news media are broadcasting the same information being sent/delivered to cell phones.

## **Consistency**

Jurisdictions need to send a consistent message to the public. It is crucial that organizations work together to ensure that all public messages are written consistently.

## Resources

*WEA Templates are in the back of this guide*

*WEA-capable Cell Phones*

This page provides a list of various wireless carriers and the WEA-capable cell phones they support.

[http://www.ctia.org/consumer\\_info/safety/index.cfm/AID/12082](http://www.ctia.org/consumer_info/safety/index.cfm/AID/12082)

CAP EAS Implementation Guide

[http://www.eas-cap.org/ecig-cap-to-eas\\_implementation\\_guide-v1-0.pdf](http://www.eas-cap.org/ecig-cap-to-eas_implementation_guide-v1-0.pdf)

# Section 2: Collaborative Operating Groups

## Section Overview

This section is to provide alerting authorities with:

- Increased awareness about Collaborative Operating Groups (COGs)—how they are issued, their structure, their capabilities, and their responsibilities
- Skills to draft appropriate, effective, and accessible warning messages using best practices in alerting

## Definition

A Collaborative Operating Group (COG) is established when a federal, state, local, tribal or territorial alerting authority successfully applies for authorization to use IPAWS. A COG may have members from multiple organizations (e.g. a regional mutual aid organization).

One of the unique features is that COGs can foster communication, collaboration, and coordination not only during the incident response phase, but also in regard to incident preparedness, mitigation, and recovery. COGs consist of, but are not limited to, organizations such as local fire departments, offices of emergency management, state police, public universities, etc.

## COG Setup Permissions

Depending on the type of access required, COGs can be set up to have the following alerting permissions:

### COG-to-COG Messaging

This configuration allows the COGs to send alert messages to each other, therefore, increasing collaboration and situational awareness of all COGs involved.

### COG-to-COG Messaging and Public Alerting

This configuration allows the COGs to send alert messages to each other and to the public, therefore, increasing collaboration and situational awareness of all COGs involved and providing members of the public with the information they need in emergency or hazardous situations.

### COG Structures

A COG may be established at any geographic level sponsored by the appropriate government agency at the federal, state, local, tribal or territorial level.

Here are some examples of COG structures:

- State
- Regional
- Single-jurisdiction
- University Level
- Multi-County

### **COG Alerting Authority**

The authority to send alerts to the public will vary based on the ways in which the COGs are established. Regions or jurisdictions may choose from a variety of governance practices:

- Some counties delegate the authority to send out the alerts to the local sublevels.
- Other jurisdictions retain the authority to approve any alerts before being sent.

### **Best Practices for COG Structures**

There is no one perfect way in which to set up a COG. COGs should be set up based on the needs and what works best for each organization.

Even within a single jurisdiction, multiple agencies such as the police department and fire department may have authority to issue alerts. When multiple agencies possess the ability to issue alerts in an area, confusion can arise from redundant or contradictory alerts. Avoiding this situation requires coordination.

Whatever the COG structure (whether regional or county), it all needs to be coordinated and supported by a Memorandum of Understanding (MOU) to show how it will work.

The MOUs and Memorandum of Agreements (MOAs) safeguard the confidentiality, integrity, and availability of the IPAWS software systems; ensure that the systems are deployed for official use only; and prevent duplicate/frivolous alerts from being disseminated to the public.

### **Relation with Governance Structure**

Alerting authorities should reference their state emergency communications (EAS) plan to govern alerting responsibilities for their state and local jurisdictions. COG permissions, including alerting jurisdictions and permissible alerting codes, should be established in accordance with established state emergency communications (EAS) plans.

# **Best Practices for COG Management**

Certain best practices are recommended for the management of a COG. A few these practices are listed below:

## **Software Compliance**

Ensure that the selected software system is in compliance with IPAWS technology.

## **Official Use**

Ensure that IPAWS-OPEN is used only in an official capacity in support of public safety (as described in the National Incident Management System).

## **Security Policies**

Ensure that appropriate security policies are in place to limit IPAWS access to authorized users (e.g. no sharing of account names and passwords).

## **System and Device Protection**

Ensure that all physical devices accessing IPAWS Open Platform for Emergency Notification (IPAWS-OPEN) receive software system-level (e.g. using up-to-date anti-virus programs) as well as physical protection.

## **Accountability**

Ensure that authorized users understand that they are accountable for their actions while using IPAWS-OPEN, and that they are required to promptly report any security incidents they encounter.

## **Rules of Behavior**

Everyone is aware of the established rules of behavior to ensure that all users have proper guidance.

## **System Interoperability**

Regular testing and contact with the State Emergency Operations Center and/or neighboring counties should be performed to ensure system interoperability.

## **Delegating Alerting Authority**

The person who signs the MOA is ultimately responsible for how the organization accesses and uses IPAWS-OPEN.

In addition, this person is also responsible for the following:

- Monitoring the actions of his/her staff members in use of IPAWS-OPEN
- Reporting incidents and/or violations of the Rules of Behavior to FEMA Security
- Reporting to FEMA discontinuation of use of IPAWS-OPEN by the Primary, Alternate, or Technical Point of Contact
- Maintaining records of personnel with access to IPAWS-OPEN

## Changing COG Permissions

When the MOA process is complete, the COG structure and points of contact are established and requested permissions are enabled. These parameters are part of a living document and can be updated as needed.

When changes are required to the COG you must contact [IPAWS@fema.dhs.gov](mailto:IPAWS@fema.dhs.gov)

## IPAWS-OPEN Access

### Granting Access to IPAWS-OPEN

Before being granted access to IPAWS-OPEN, each user must:

- Complete the [IS-247.a-IPAWS](#) web-based training. In addition, it is recommended that users also complete training and materials that are specific to their organization.
- Receive training from their alert origination software provider to train their staff to ensure they know how to appropriately use the software and manage its capabilities.
- Where applicable, document and maintain records of successful completion of FEMA-required training and produce such documentation in response to official inquiries and/or requests.
- Read, understand, and sign the *IPAWS Rules of Behavior*. *Rules of Behavior* help staff members understand that the IPAWS-OPEN system:
  - Is for official use only
  - Requires users to create user ID and passwords based on the provided guidelines.

## **Managing Level of Access to IPAWS-OPEN**

Emergency Managers or the person(s) in charge of IPAWS-OPEN at the COG should ensure that users are provided the appropriate level of access to IPAWS-OPEN commensurate with their roles and authority.

The level of access to IPAWS-OPEN and access to the system is granted in a variety of ways including the most common ways of either:

- The user's position in the organization
- The individual's name in the organization

## **Monitoring Access to IPAWS-OPEN**

When users sign the *IPAWS Rules of Behavior*, they acknowledge that they will be accessing the system for official use only. However, the responsibility for the release of individual alert messages falls on the IPAWS COG System Owner who is responsible for anyone with access to the IPAWS-OPEN system under that COG ID. Remember that just because someone has administrative rights to the system, it does not mean that he/she may send an alert message at will.

FEMA IPAWS knows when a COG issues a message to IPAWS-OPEN; however there is no way for FEMA IPAWS to know which individual user of the COG issued the message. The COG system owner should have the means to audit users' access to the system as well as their activities while logged in. FEMA reserves the right to disable a COG if anyone in the COG violates the Rules of Behavior.

## **Identification of the Originator**

Some hardware based systems have an eight (8) character limit identifying your organization. In the equipment setup be aware if there is a limitation and what can be done to make your organizations name clear as you issue alerts to the public. Use the following recommendations to identify the agency;

**State Agency, Region, County and City ID** should use the first 3 or 4 characters of name to ID that origination location source

Minneapolis = MPLS

St. Paul = StP

Ramsey = Ram

Rochester = Roch

Department of Public Safety, Division of Homeland Security and Emergency Management = MN HSEM

Department of Public Safety, Bureau of Criminal Apprehension (BCA) = MN BCA

**Use these acronyms for the service.**

Sheriff's Office = SO

Public Safety Answering Point = PSAP

Emergency Management & Homeland Security = EMHS

Emergency Management = EM

Homeland Security = HS

## Resources

Select each link below to learn more about additional resources.

### **IPAWS Toolkit for Alerting Authorities**

The IPAWS Toolkit, developed by the IPAWS office, provides alerting authorities at all levels of government with resources to assist them with the adoption of Common Alerting Protocol (CAP), incorporate IPAWS, and ensure their communities understand how to access, use, and respond to public alert and warning information. It can be accessed by selecting this link:

<http://www.fema.gov/informational-materials>

### **Alerting Authorities**

This web page provides useful information on IPAWS for alerting authorities. It can be accessed by selecting this link: <http://www.fema.gov/alerting-authorities>

## Points of Contact:

John Dooley  
Division of Homeland Security and Emergency Management  
Minnesota Department of Public Safety  
445 Minnesota Street, Suite 223  
St. Paul, Minnesota 55101-6223  
Phone Number 651-201-7498  
Email [john.dooley@state.mn.us](mailto:john.dooley@state.mn.us)

Scott A. Williams  
Director of Emergency Communications  
Ramsey County Emergency Communications Center  
388 13th Street  
St. Paul, MN 55101  
Phone Number 651-266-7721  
Email [scott.williams@co.ramsey.mn.us](mailto:scott.williams@co.ramsey.mn.us)

## Wireless Emergency Alert Worksheet

Remember 90 characters are all you have to work with free form.

Source	Guidance	Hazard	Location	Termination Time
--------	----------	--------	----------	------------------

1	2	2	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90

**Authorized Event Code:**

**Authorized Code    Code Description**

- CDW                      Civil Danger Warning
- CEM                      Civil Emergency Message
- EVI                        Evacuate Immediately Warning
- SPW                      Shelter in Place Warning

**What priority codes should be assigned?**

**Urgency**

**Severity**

**Certainty**

- |                                    |                                   |                                   |
|------------------------------------|-----------------------------------|-----------------------------------|
| <input type="checkbox"/> Immediate | <input type="checkbox"/> Extreme  | <input type="checkbox"/> Observed |
| <input type="checkbox"/> Expected  | <input type="checkbox"/> Severe   | <input type="checkbox"/> Likely   |
| <input type="checkbox"/> Future    | <input type="checkbox"/> Moderate | <input type="checkbox"/> Possible |
| <input type="checkbox"/> Past      | <input type="checkbox"/> Minor    | <input type="checkbox"/> Unlikely |
| <input type="checkbox"/> Unknown   | <input type="checkbox"/> Unknown  | <input type="checkbox"/> Unknown  |

Fill in codes on back side also.

# Wireless Emergency Alert Worksheet

**Response Type: (some programs insert this automatically based off the event code)**

<b>Response Code</b>	<b>Code Description</b>
<input type="checkbox"/> Evacuate	Relocate as per instructions
<input type="checkbox"/> Prepare	Make preparations as per instructions
<input type="checkbox"/> Execute	Execute a pre-planned activity as per the instructions
<input type="checkbox"/> Avoid	Avoid the subject event as per the instructions
<input type="checkbox"/> Monitor	Attend to information sources as per the instructions
<input type="checkbox"/> Access	Evaluate the information in the message
<input type="checkbox"/> All Clear	The subject event no longer poses a threat or concern
<input type="checkbox"/> None	No Action recommended

**WEA Category: (some programs insert this automatically based off the event code)**

<b>Category</b>	<b>Description</b>
<input type="checkbox"/> Geo:	Geospatial (including Landslides)
<input type="checkbox"/> Met:	Meteorological (Including Floods)
<input type="checkbox"/> Safety:	General Emergency and Public Safety
<input type="checkbox"/> Security:	Law enforcement, Military, Homeland and Local security
<input type="checkbox"/> Rescue:	Rescue and Recovery
<input type="checkbox"/> Fire:	Fire Suppression and Rescue
<input type="checkbox"/> Health:	Medical and Public Health
<input type="checkbox"/> Env:	Pollution and other environmental
<input type="checkbox"/> Transportation:	Public and Private transportation
<input type="checkbox"/> Infra:	Utility, telecommunication, other non-transport infrastructure
<input type="checkbox"/> CBRNE:	Chemical, Biological, Radiological, Nuclear and High Yield Explosive
<input type="checkbox"/> Other Events	

## Standard Operating Procedure (SOP) for

### Testing with the IPAWS Lab at the Joint Interoperability Test Command (JITC)

Instructions are prepared under the assumption that an active Memorandum of Agreement (MOA) is in place between the FEMA IPAWS Program Management Office and Alerting Authority.

#### 1. On-Site Testing:

- Alerting Authority contacts the JITC Point of Contact (POC)
- Alerting Authority and JITC POC coordinate dates to visit the lab
- JITC POC provides Navy vetting documents and instructions to the Alerting Authority (if required)
- Alerting Authority completes and submits vetting documents to the JITC POC; the JITC POC will review and then forward to JITC Security
- Alerting Authority ensures the JITC endpoint and JITC security certificate are uploaded to the alert origination tool [https://www.ipaws-open.net/IPAWS\\_CAPService/IPAWS](https://www.ipaws-open.net/IPAWS_CAPService/IPAWS)
- Alerting Authority determines a testing agenda
- Alerting Authority drafts requirements, scenarios, test scripts, etc.
- JITC configures EAS devices in accordance with Alerting Authority Collaborative Operating Group (COG) permissions

#### 2. Off-Site Testing (via webinar):

- Alerting Authority contacts the JITC POC
- Alerting Authority provides 2-3 test dates and times (typically 1 hour)
- JITC schedules a webinar and provides link and teleconference number to the Alerting Authority
- Alerting Authority ensures JITC endpoint and JITC security certificate are uploaded to alert origination tool [https://www.ipaws-open.net/IPAWS\\_CAPService/IPAWS](https://www.ipaws-open.net/IPAWS_CAPService/IPAWS)
- Alerting Authority coordinates webinar attendees (e.g., vendor and/or colleagues) JITC configures EAS devices in accordance with Alerting Authority COG permissions

#### 3. Independent Testing:

- No need to notify JITC POC
- Alerting Authority ensures JITC endpoint and JITC security certificate are uploaded to alert origination tool [https://www.ipaws-open.net/IPAWS\\_CAPService/IPAWS](https://www.ipaws-open.net/IPAWS_CAPService/IPAWS)
- Alerting Authority verifies test alerts via the IPAWS Message Viewer: [https://ipaws-open.net/ALERT\\_SERVICES/postedmessages.php?COGID=15XXXX](https://ipaws-open.net/ALERT_SERVICES/postedmessages.php?COGID=15XXXX)

#### JITC POC:

---

Jody Smith  
Manager, IPAWS Lab  
JITC  
3341 Strauss Avenue, Building 900  
Indian Head, MD 20640  
301.743.4267 (direct)  
301.743.4354 (lab)  
[Jody.m.smith20.ctr@mail.mil](mailto:Jody.m.smith20.ctr@mail.mil)

Stan Eckert  
Action Officer  
JITC  
3341 Strauss Avenue, Building 900  
Indian Head, MD 20640  
301.743.4267 (direct)  
301.743.4354 (lab)  
[William.s.eckert.civ@mail.mil](mailto:William.s.eckert.civ@mail.mil)

**Notes:** \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_