2020

Statewide Alert, Warning and Notification Best Practices Guide

VERSION 2.0

SECB

Alert System (EAS or WEA) Checklist for Alert Originators

In general, the following conditions should be considered in determining whether the issuance of an EAS or a WEA is warranted:

EAS / WEA Activation Checklist

Yes No

___ ___ Is this a sudden, unforeseen or unpredictable situation?

___ ___ Does the situation pose an imminent threat to life or property?

___ ___ Does the situation have the potential to adversely affect a significant population or geographic area?

___ ___ Does the situation require that the public be told immediately to seek shelter or take other protective action?

___ ___ Are other means of disseminating information inadequate to ensure rapid delivery of the information?

Important: Do not activate EAS or WEA if the answer to any of these questions is “No.”

Contents

Preface: This document describes the recommended best practices, standards 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 (IPAWS).

Document Revision History

Date of Revision	Revision Number	Person(s) Responsible for Revision	Changes Made
9/17/2020	2.0	John Dooley Lindsey Broda Brandon Benjamin	All new material.
4/16/2021	2.01	John Dooley	Addition of FEMA Help desk Information on page 41.

Executive Summary

A comprehensive alert and warning program is a critical component of a community’s ability to effectively respond to emergencies. The state of Minnesota identified the need to establish statewide guidelines for enabling and encouraging consistent application of alert and warning best practices, procedures and protocols.

The safety of local communities requires designated alerting authorities to ensure they have multiple trained alert originators, adequate training, testing and functional equipment or software.

This Statewide Alert, Warning and Notification Best Practices Guide was developed in collaboration with a group of local, state, federal, tribal and private partners that are part of the Statewide Emergency Communication Board (SECB) IPAWS committee.

The document provides guidance and expectations for jurisdictions with designated alerting authorities for implementing an alert, warning and notification program within the state of Minnesota. Additionally, the document provides overarching direction to the sub-components of the statewide alert and warning system, including the State EAS, sub-jurisdictional alert, and local alert and warning notification plans.

Purpose

The Statewide Alert, Warning and Notification Best Practices Guide describes the recommended best practices, standards and assist jurisdictions with writing templates and managing their mass notification systems in regards to usage with IPAWS.

Intended Audience

The intended audience for this document is personnel from the agencies and jurisdictions within the State of Minnesota that have a role in notifying the public effectively before, during and after emergencies so that protective actions can be taken.

What are Public Alerts, Warnings and Notifications?

Type	Timeframe	Purpose	Examples
Warning	Prior to incidents.	Distribute guidance to prepare for an anticipated incident.	Weather watches/warnings, fire warnings, evacuation orders.
Alerts	At the beginning of and during incidents with ongoing, immediate threats.	Gain the attention of the public and draw their attention to a risk or hazard.	Active shooter and other dangers, hazardous materials concerns, 911 outages, AMBER alerts.
Notifications	During and after immediate threats.	Instruct immediate protective actions and provide ongoing communications relevant to an event to reduce milling and encourage public action. Convey time-sensitive information on response- and recovery-related services.	Protective actions, evacuation routes, boil-water advisories, return-from-evacuation notices, area-accessibility updates.

Elements of an Alert, Warning and Notification Program

The alerting ecosystem continues to evolve as new technologies are introduced and new practices and protocols for information sharing emerge during emergency events. An understanding of alerting implementation best practices lays the foundation for alert originators to examine and determine effective combinations of alerting tactics for their own jurisdictions. The following sections outline best practices that alert originators have highlighted as improving overall public response, regardless of incident type.

Clear Delegation of Authority

Alert originators typically use internal, self-created standard operating procedures (SOPs) or other guidance documents to help define alerting authorities and varying levels of administrator rights. Having a clear delegation of authority enables quicker decision making by streamlining processes and minimizing confusion within an alerting authority. When employees clearly understand what is expected of them, it speeds up the process of sending an accurate alert. SOPs that outline safeguards in the chain of command also reduce errors that may cause public confusion, delayed public response, and degraded trust in alerting systems.

Public Education

Public education about alerts, warnings and notifications before any incident helps communities nationwide understand their purpose and importance and minimizes confusion. The public needs to know what to expect from alerting tools and what actions they might need to take. Continuous public education is a critical, ongoing task that expedites and encourages public protective actions.

Public Education Tips

Alert originators must educate the public ahead of an incident to reduce confusion and increase alert effectiveness. Alert originators who have successfully educated the public and seen results identified the following tactics to improve awareness:

- Conduct localized, public tests of alert systems to increase public familiarity.

- Share general information about alerting systems year-round over multiple channels (e.g., events, social media) to increase public awareness and opt-in subscriptions.

- Target specialized education and outreach campaigns ahead of major events (e.g., preparedness events, scheduled tests and rollout of a new alerting tool).

- Leverage existing regional and state organizations that support emergency response coordination to conduct education and outreach efforts. For example, the development of coordinated social media kits with resources (e.g. templates, canned language) for recurrent or planned incidents (e.g., Tornado Awareness Week, National Preparedness Month, Winter Weather Preparedness Week, etc.).

- Partner with trusted community networks (e.g., faith-based institutions, schools, neighborhood associations) to build trust and distribute educational materials. When possible, send a representative to attend community meetings.

- Partner with major businesses in your area to conduct regular education sessions. Businesses often require emergency planning sessions as part of Human Resources functions.

Training and Exercise

Preplanned exercises provide an excellent opportunity to use alert and notification systems. A major exercise may affect the public and require an alert of 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 Collaborative Operating Group (COG) for training and exercises. This test COG can be programmed into many IPAWS authoring tools as a separate distribution environment. This allows users to create and send messages to a test environment without alerting the public.

Use of Templates and Pre-Approved Language

Predesigned alerting templates and pre-approved language minimize the chances for error and enable alert originators to disseminate important messages quickly. Alert originators should craft pre-scripted "fill in the blank" message templates before an incident for all hazards they face regularly. Additionally, alert originators create templates for other regular protective action advisory messages, such as prepare to evacuate, shelter in place, and hazard awareness.

The Guidelines for Issuing Public Alerts and Warnings (see page 13) covers common hazards, explains how to respond when certain incidents or thresholds occur, and suggests what to include in a message or provides pre-approved language. All authorized originators are trained on the matrix and use it for incidents.

For templates to be successful without delaying alerts and notifications, they must be integrated into day-to-day operations. By identifying common incidents and encouraging use, the originator shouldn't have to rely on one person to put out the alert.

Alerting and Usage

Training and routine tool use allows alert originators to practice alerting procedures and gain familiarity with alerting technologies to minimize errors during an incident. Every incident is different, with varying factors and decision points that change in a matter of seconds. It is critical to train staff on not only how an alert is transmitted, but the effects of the alert on the public, to encourage high-impact alerting. Conducting regular internal tests in a controlled and closed environment, such as through the FEMA IPAWS Test Lab, will help maintain that proficiency. See Proficiency Demonstration in Section 3 for more details.

Applying Lessons Learned

Alerting authorities should review and update alerting practices on a regular basis and not wait for a large incident to occur to identify gaps in alerting systems, platforms and/or technologies. Additionally, alerting tactics and procedures should be examined together, as opposed to separately and at regular intervals to maximize effectiveness and overall public reach. Local alert originators are invited to enhance information sharing, increase coordination and discuss potential enhancements to operations. This is an opportunity to get feedback on system use and identify possible improvements. Alerting authorities should also consider ways to incorporate feedback and lessons learned from the public.

Measure Alert Effectiveness

The primary measure for determining if an emergency alert is successful is whether or not the public takes appropriate action. Feedback is needed during a crisis to immediately understand how the public is responding to the event so that systems can be improved. Alert originators that regularly and successfully measure alert effectiveness will improve public response.

Access and Functional Needs

Individuals with access and functional needs may require alerts in varying formats. An example of an IPAWS initiative to improve accessibility is the symbology designed in collaboration with the National Alliance for Public Safety GIS (NAPSG). The following elements will improve accessibility:

- Clear and plain language.
- Text-to-speech conversion.
- Consistent audio.
- Ample text and audio to explain images/maps.
- Screen reading and text-to-speech devices.

Alerting administrators should keep in mind the needs of persons with access and functional needs in their community. It is best to use clear and plain language whenever possible, with minimal use of abbreviations. The most important information should be presented first. Care must be taken in composing text that is converted to audio by text-to-speech equipment. The audio should be as consistent as possible with the text and should ensure that any abbreviations are spoken as full words.

Because IPAWS Open Platform for Emergency Networks (OPEN) provides the capability to deliver multimedia messages, ample text and audio should be provided to explain images or maps so that message recipients can understand what is being conveyed graphically.

Some wireless devices and currently available software provide screen reading and text-to-speech conversion capabilities for alerts delivered via Internet technologies. When considering these and other translation technologies, craft messages that avoid nonstandard language formats and terminology.

Roles and Responsibilities of Government

Federal

Federal Emergency Management Agency (FEMA) is the lead federal agency for coordination and implementation of IPAWS. FEMA ensures that this nationwide system is maintained and operational. FEMA’s stated goals for IPAWS are to:

- Issue the COG ID, enter in to an IPAWS memorandum of agreement (MOA) with the jurisdiction and issue certificates to the jurisdiction.
- Partner with National Oceanic and Atmospheric Administration (NOAA) for seamless integration of message transmission through NWS national networks.
- Facilitate dissemination of Presidential Alerts during a national emergency.
- Receive and authenticate alert messages, then delivers to all IPAWS-compliant public alerting systems.

Federal Communications Commission (FCC) works with EAS participants and cellular providers for proper planning and administration of EAS and WEA activities.

National Weather Service (NWS) has responsibility for originating public warnings regarding weather hazards. While the NWS has responsibility for weather-related alerting, local government is not precluded from sending notifications and alerts in support of weather events.

National Weather Radio (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.

- As of the publishing date of this guide, there are no authorized Minnesota COGs that can send an alert through the FEMA IPAWS OPEN system to the NWS system.
- 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.

State

Department of Public Safety (DPS) is the main public alert and warning responsibility of the state, even though all disasters emerge on a local level.

- **Emergency Communication Networks (ECN):**
    - Provides training, consultation and guidance on alert and warning standards.
    - Provides best practices to local government entities.
    - Establishes access to and uses available urgent communications tools, such as the federal IPAWS network.
- **Bureau of Criminal Apprehension (BCA)** serves as a central point for validating the requests for and issuing both Child Abduction Emergency (AMBER) and Law Enforcement (Blue)) alerts**.**
- **Homeland Security and Emergency Management (HSEM) s**erves as the primary message issuer for nuclear power plant warnings with the BCA serving as backup.

Tribal

Tribal communities are essential components of our nation’s emergency management team. The IPAWS Program Management Office (PMO), in adherence with FEMA's Tribal Policy, supports nation-to-nation tribal relationships and recognizes the unique cross-jurisdictional challenges tribal nations face with emergency management and public alerting.

To enhance the preparedness of tribal governments and their working relationship with FEMA, the IPAWS PMO collaborates with tribal emergency management. The purpose is to facilitate communication through tribal conferences and tribal associations, providing outreach and training opportunities to stakeholders.

Tribal nations’ alerting plans are not subject to state review or approval by local authorities. As sovereign nations, tribal governments are encouraged to coordinate alert plans with surrounding jurisdictions.

Local Jurisdictions

Keep public informed about natural, human-caused and technological disasters in addition to the actions they need to take to protect themselves and their families. Depending on the organization of local area governments and coordination of the local area alert and warning system, the local government responsibility may include city, special district, county and multi-county jurisdictions.

- Local government officials typically have the most accurate and timely understanding of the situation, necessary protective actions, and potential adverse impacts of the incident.

- Local officials need to rapidly and adequately communicate to the public what is occurring and any steps or actions the public needs to take.

Governance: Law, Policy and Regulations

Law

Public Law 114-143, The IPAWS Modernization Act.

Public Law 93-288, The Stafford Act, Sec. 202

Policy

Executive Order 13407 – Public Alert and Warning Systems

Regulation

47 CFR Part 10 – Wireless Emergency Alerts

47 CFR Part 11 – Emergency Alert System

MN State Statute 12.03, Subd. 4. Emergency management.

Section 1: When to Issue an Alert, Warning or Notification

Overview

This section introduces you to factors and guiding principles of alerts, warnings and notifications, including:

- Criteria for issuing.
- Social factors that may influence alerts and warnings.
- Alert message requirements.
- Guidelines for issuing alerts and warnings.

Alerts and warnings should be issued when there is an imminent threat to life, health or property. This can include alerts and warnings issued in advance of forecasted severe weather events when doing so will give the public time to evacuate or take cover. When a threat exists, even though it might not be imminent, such as a hazardous chemical release or flooding, best practice is to communicate that threat to the public so that they may be better prepared. Warning systems such as sirens, while helpful in alerting a community to a hazard, should not be used for reassuring the public that an ongoing situation or an upcoming event is not hazardous; other public information channels (Facebook, Twitter, radio and others) should be used for those purposes instead.

Fear of triggering panic is not a valid reason to delay or avoid issuing a warning. Mass panic very rarely occurs as the result of a warning message. Note that justified anxiety or physical flight is not the same thing as panic. When public warning information is delivered by a credible alerting authority, the public usually responds by following the recommended actions. Rarely do such warning messages lead to mistrust or panic.

When dealing with uncertain or conflicting information about a threat, the alerting authority should err on the side of protecting the public. Some warning systems have provisions for communicating the general degree of certainty associated with threat information, but many only permit a yes-or-no decision as to warning the public. Reasonable detail should be provided, but a warning message is not the place for an extended discussion of scientific data and probabilities.

Irrelevant warnings can fatigue the public rapidly and lead to recipients discounting further warning messages or opting out of receiving future alerts and warnings. Every effort should be made within the capabilities of the warning system to limit the warning to people actually at risk. Warning systems become more effective to the extent they can target limited areas or specific at-risk populations.

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:

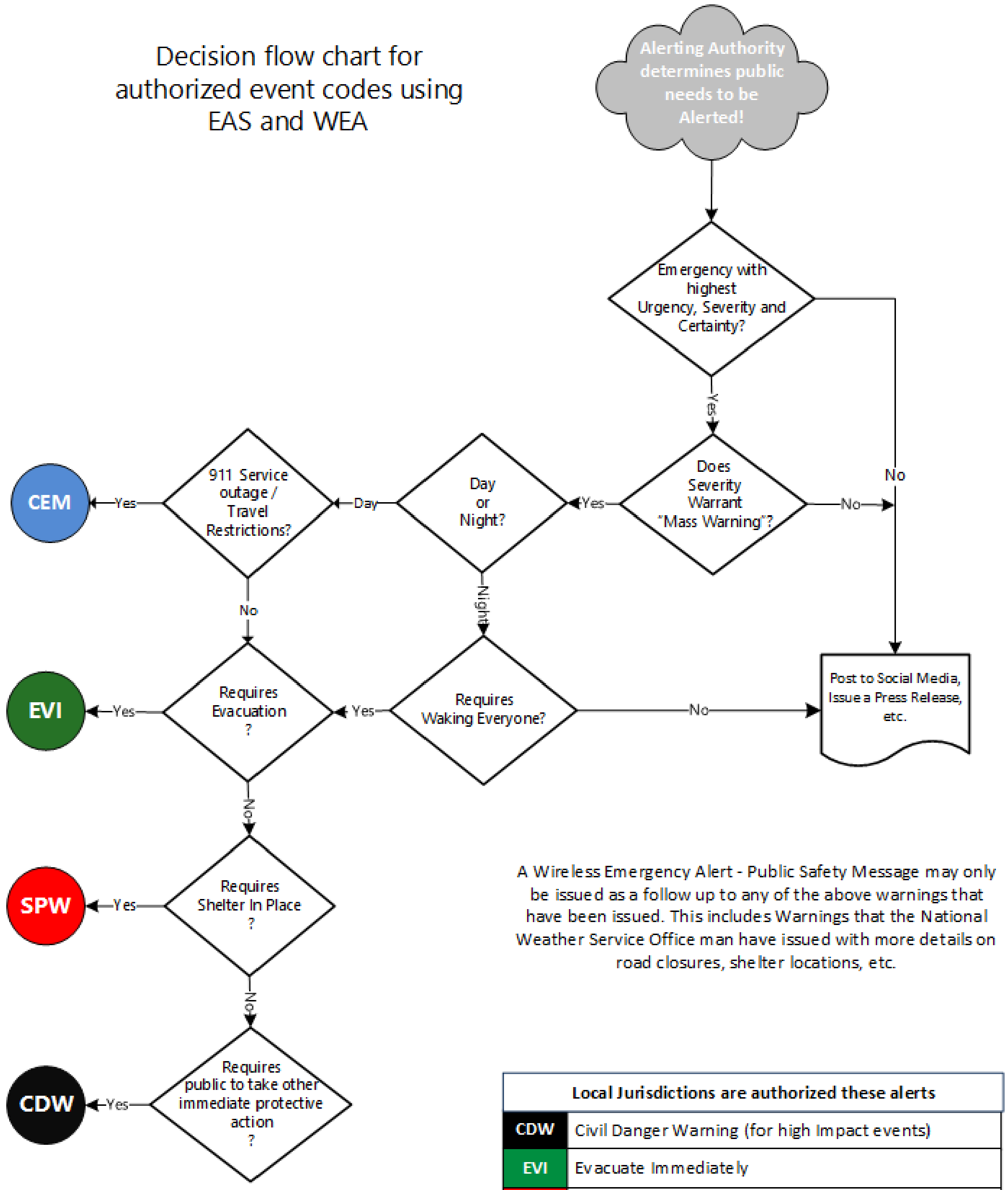
- Does the hazardous situation require the public to take immediate action?
- Does the hazardous situation pose a serious threat to life or property?

- 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?

The following flow chart is an example of how a decision to send out an alert or warning could go.

Minnesota

Decision flow chart for authorized event codes using EAS and WEA



Alerting Authority determines public needs to be Alerted!
Emergency with highest Urgency, Severity and Certainty?
Yes
No
Does Severity Warrant "Mass Warning"?
Yes
No
Day or Night?
Day
Night
911 Service outage / Travel Restrictions?
Yes
No
CEM
Requires Waking Everyone?
Yes
No
Post to Social Media, Issue a Press Release, etc.
Requires Evacuation ?
Yes
No
EVI
Requires Shelter In Place ?
Yes
No
SPW
Requires public to take other immediate protective action ?
Yes
CDW

A Wireless Emergency Alert - Public Safety Message may only be issued as a follow up to any of the above warnings that have been issued. This includes Warnings that the National Weather Service Office man have issued with more details on road closures, shelter locations, etc.

Local Jurisdictions are authorized these alerts	
CDW	Civil Danger Warning (for high Impact events)
EVI	Evacuate Immediately
SPW	Shelter In Place Warning
CEM	Civil Emergency Message (for priority information)

Social Factors that Influence Alerts and Warnings

Several social factors also influence the extent to which alerts and warnings are received, comprehended and heeded. These factors include:

Personal Dynamics

Personal dynamics require the individual to adapt and adjust in their environment to the situation at hand.

Level of Community Interaction

People with a higher level of engagement in the community will receive more warnings and are therefore more likely to act.

Confirmation

Individual responses to warnings vary, but many people will seek some form of confirmation. For example, some people will look for more information through environmental cues, while others will seek to contact other trusted sources. Optimism bias (thinking that "disasters happen to other people") may be overcome with confirmation.

Perception of Risk/Proximity

People tend to make a rapid assessment of the relative safety of their location, producing an emergent perception of risk. If their perception of personal risk is high, people will act quickly. When the perception is low, they will delay acting.

Length of Residency

Transients, tourists and newcomers to the area lack knowledge of local hazards and the history of local disasters, so they may react differently.

Language

Non-English-speaking persons may not understand warnings provided in English. Communities with high percentages of non-English-speaking people should issue warnings in the primary language(s) of the population as well as in English.

Family Composition

Families, more than individuals, tend to heed evacuation warnings. Their decisions are based on the following factors related to family composition:

- Family network: People are more likely to act if they have relatives nearby who may warn them and offer them short-term shelter.
- Presence of children: Concern for children's safety will elicit quicker response from parents.
- Presence of pets: People often view their pets as members of their family and will prioritize their safety in emergencies. People with pets may endanger their own lives by refusing to evacuate, because many public shelters do not allow pets.

Other personal dynamics also have an influence on the extent to which alerts and warnings are received, understood and heeded.

Previous Experiences

People will often rely on their previous experiences with the hazard to determine what actions they initially take or don't take. For example, if they have evacuated for flood warnings in the past and it never occurred, then they may be less willing to evacuate in the future.

Translation of Notifications

The state of Minnesota is composed of many diverse communities, some of which include non-English-speaking populations. Identifying the most commonly used languages and having a process in place to translate warning messages will ensure the greatest number of residents receive the warnings. It is important, however, to not let the inability to translate a message delay notification when time is of the essence and lives are at risk. Reduce reliance on free digital translation services, as they can often misinterpret the message. Where feasible, contract with translation services, such as local translators and/or telephonic interpretation services. Then verify with community members for proper dialect.

Culture

Due to the rich cultural diversity in Minnesota, communities may respond to an alert's messaging in different ways. For example, some communities may respond negatively to instructions from the government. Prior to an incident, it is important to locate trusted agents within communities who can help convey the intended meaning of a message and educate the affected community on the jurisdiction's alert and warning program. This may include religious leaders, non-profit agency representatives, local elected officials or prominent business owners within the respective community. Leveraging the relationships that have been established with these leaders will be a force multiplier when the time comes for a warning to be communicated to the community.

Alert Message Requirements

There are four classes of Alert Messages:

- The Presidential Alert is issued by the President of the United States or the President's authorized designee. Users cannot turn off this category.

- The Child Abduction Emergency/AMBER Alert is initiated in Minnesota only by the Bureau of Criminal Apprehension (BCA) based on the U.S. Department of Justice's three criteria, which should be met before an alert is activated. See the BCA AMBER Alert web page for procedures. Users have the option of turning this alert off.

- The following two alert classes are available to properly authorized jurisdictions:

    - An Imminent Threat Alert notifies the public of a life safety or property damage hazard that meets a minimum value for each of three CAP elements: urgency, severity and certainty. Users have the option of turning this alert off.

- A Public Safety Message is an essential advisory that prescribes one or more actions likely to save lives and/or safeguard property during an emergency. A Public Safety Message may only be issued in connection with an Imminent Threat Alert Message. Users have the option of turning this alert off.

The following table shows the levels of urgency, severity and certainty (those in red will trigger a WEA alert):

Urgency	Severity	Certainty
Immediate Responsive action should be taken immediately	**Extreme** Extraordinary threat to life or property	**Observed** Determined to have occurred or to be ongoing
Expected Responsive action should be taken soon (within next hour)	**Severe** Significant threat to life or property	**Likely** Likely (more than 50% chance)
Future Responsive action should be taken in the near future	**Moderate** Possible threat to life or property	**Possible** Possible but unlikely (less than 50% chance)
Past Responsive action is no longer required	**Minor** Minimal to no known threat to life or property	**Unlikely** Not expected to occur
Unknown Urgency unknown	**Unknown** Severity unknown	**Unknown** Certainty unknown

The following table shows alerts, warnings and notifications for various situations.

The Distribution Method(s) column features recommendations of ways to distribute your message. You don’t have to use them all.

Guidelines for Issuing Public Alert and Warnings

Situation	Distribution Method(s)	Recommended IPAWS Code	Message Circumstances
Life Safety High Priority, High Risk Incident	IPAWS - EAS IPAWS - WEA Mass Notification System Social Media Media Release	Civil Danger Warning (CDW)	• Active shooter • Dam breach • Large, escalating hazardous materials • Pipeline • Water supply contamination
Requiring Evacuation	IPAWS - EAS IPAWS - WEA Mass Notification System Social Media Media Release	Evacuation Immediate (EVI)	• Flooding • Dam breach • Hazardous materials • Wildfire
Requiring People to **Stay Where They Are**	IPAWS - EAS IPAWS - WEA Mass Notification System Social Media Media Release	Shelter-In-Place (SPW)	• Hazardous materials • Environmental health hazard (e.g. Air quality)
Priority Information	IPAWS - WEA Mass Notification System Social Media Media Release	Civil Emergency Message (CEM)	• 911 service disruption • Emergency closure of major roadways • No travel advised • Location of confirmed NWS-issued warnings
Priority Public Safety Information to **Follow Up on Previous Alert**	IPAWS - WEA Mass Notification System Media Release	Public Safety Message	• Awareness/Impact – Following NWS- issued alert (e.g. areas to avoid, detours) • Awareness/Impact – Following CEM (e.g. downed power lines, road closure, shelter locations)
Prepare for Expected Event/ Post-Event General Information	Mass Notification System Social Media Media Release	Electronic Telephone Notification (ETN)	• Community preparedness message • Town hall meeting • Generalized public safety message
System Test	IPAWS – EAS IPAWS - WEA	Required Weekly Test (RWT)	• Conduct end-to-end test without public alert

Timeframes for Issuing Alerts and Warnings

Agencies should maintain an alerting capability at all times, if possible by maintaining a primary operational capability, as well as a back-up capability for use when the primary capability is not functioning or inaccessible. Maintaining the capability to send out an alert is imperative as disasters may strike at any time and jurisdictions are responsible for informing the public in a timely manner of the threat and protective actions to take.

Agencies should issue alert and warning messages as soon as feasible given the circumstances. Access to the designated alerting authority and alerting originator should not be delayed due to limited resources or non-operational equipment. Designated alerting staff should have ready and reasonable access to primary or backup alerting systems and be properly trained and well-versed in operating the equipment.

Guidelines

The impact area is the geographic area 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., search for an armed suspect) that affects a few blocks.
- Community-wide event: An event (e.g., hazmat incident) that affects a major part of a small jurisdiction.
- Multi-community event: An event (e.g., a tornado) that affects several communities within an area.
- Regional event: An event (e.g., a nuclear power plant event) that affects an area encompassing many jurisdictions and requires assistance from state-level entities.

When to Issue Alert and Warnings

To ensure an effective alert and warning program, a jurisdiction should closely coordinate and collaborate with all public safety agencies within the jurisdiction and neighboring communities to develop a shared understanding of the local alert and warning plan prior to an incident and specific alert and warning actions taken during an incident.

To the extent possible, alert and warning messages should be distributed to all members of the community who are at risk, including commuters, travelers or transient populations, people with disabilities or access and functional needs, non-English speakers, people in remote or isolated areas, the elderly, and people with limited technology. Additionally, when providing emergency alerts and notifications, it is vital to note that local, state and federal governments are keenly aware that not everyone receives or processes information in the same manner. The Americans with Disabilities Act (ADA) requires jurisdictions to make all information accessible to their constituents, including emergency alerts and warnings. As such, governments must account for the access- and functional-related needs specific to alerts and warnings that impact all individuals, including those who are deaf or hard of hearing, blind or low vision, or non-English speaking; persons with intellectual or developmental disabilities; or any others who receive and/or process information in different ways. Emergency alerts and warnings should help fulfill the wide array of communication needs of the public.

In some cases, it may be useful to offer alternative protective action recommendations for people who cannot implement the preferred recommendation, such as those with physical disabilities or medical conditions, or those without access to transportation. Also, as it may take longer for these populations to respond to a warning, earlier "pre-warnings" directed to them may be useful. However, initial warnings should not be delayed while alternate versions are being prepared. Translations or other variants of a warning message should be treated as updates.

People rarely act on a single warning message alone. To be effective, warnings should be delivered in various formats across multiple media platforms, both to increase reliability of warning delivery and to provide a sense of corroboration that will encourage recipients to take protective actions. Each community may have multiple methods to send out warning messages, and each of these tools should be used with similar messages to ensure that the greatest number of individuals in communities receive the messages. When sending out messages, coordination among the jurisdictions within the impacted area is important to reduce confusion and ensure contradictory messages are not being sent.

Message Library

Jurisdictions are encouraged to establish a message library with sample messages that have been translated into the languages most commonly used in the communities they serve. Pre-planned messages can save time in a disaster and ensure that accurate translations exist for messages that are critical for the community.

Shapefiles of cities, industrial facilities, and sporting venues can be placed it this category. There may come times that you need to clear a certain area; these shapefiles may be a great time saver.

Section 2: How to Warn — 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:

- Characteristics of an Effective Alert Message
    - Source
    - Guidance
    - Hazard
    - Location
    - Termination Time
- Use of Templates – WEA
- Use of Templates – EAS
- Use of Social Media

Characteristics of an Effective Alert Message

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:

- Specific — about what you're asking the public to do and be accountable for.
- Consistency – within messages and from one message to the next.
- Certainty — tell them the possibilities.
- Clarity — use clear language and avoid unnecessary abbreviations.
- Accuracy — what they should know from the government

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:

- Use clear and simple language.
- Avoid non-standard language to facilitate easier text-to-speech conversion and use of screen reading devices.
- Ensure consistency of audio with message text.
- Provide ample text and audio to explain images/maps.

English as a Second Language

The FEMA IPAWS OPEN aggregator does not provide translation services, but it is capable of accepting and relaying alerts in multiple languages as composed by the alerting authority. 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 to minimize the amount of information requiring translation for actual alerts.

Five key elements of a message and the information they should include:

Message Element	Element Description
Source	Who is the message from? Your citizens want to know if the message is from an authoritative source. Shorten the name of your organization when needed for messages with limited space (e.g. IPAWS 90-character legacy or SMS). If your mass notification system can automatically provide the source information through a customized caller ID and custom audio (for phone messages), as well as for SMS and email messages, you should only need to add the Source for IPAWS and other certain types of messages.
Hazard	What is the danger? While you can create a generic message, a specific template for the most common hazards in your area (e.g. floods, wildfires, boil-water alert, etc.) will be helpful. Include relevant location and time parameters in either the hazard or guidance description when needed.
Guidance	What should the recipient do? Be brief and use standardized words for guidance, as the code you choose does not show up in the message display in WEA automatically. Use words and phrases such as "evacuate," "take shelter," "shelter in place," and “check for updates” (if you are pointing them to a web page, etc.; if time permits, you can add more situation-specific information).
Location	Where is the hazard? When using this, you'll fill in a description of the place, using language the recipient will understand. NOTE: If using a polygon, do not exceed 10 polygons or 100 points, as it will cause your message to be rejected at the IPAWS OPEN Server. Square polygons are acceptable; the simpler, the better.
Termination Time	When is the hazard expected to be over or no longer relevant? This only applies when the information is available and you want to publish it in the message. You might also plan on using "unknown" to fill in a template. Note: WEA requires a termination time and cannot go past 24 hours, as it will keep broadcasting your message to phones that continue to enter your polygon until the message termination time has arrived. Once a phone receives that message, it sees all other instances as duplicates unless you have posted an UPDATE.

Source

- Who is the message from?
- Your citizens want to know if the message is from an authoritative source.
- Who or where do they go to for more information if necessary.

Note: You'll want to shorten the name of your organization when needed for messages with limited space (e.g. IPAWS 90-character legacy or SMS.)

Guidance

The FCC established naming conventions for EAS event codes. In most cases and for all future codes to be approved, the third letter of all hazard event codes is limited to one of two letters, with a few exceptions: Evacuation Immediate (EVI) other examples; Civil Danger Warning (CDW) or Child Abduction Emergency (CAE).

Warning	An event that alone poses a significant threat to public safety and/or property, probability of occurrence and location is high and the onset time is relatively short.
Emergency	An event that, by itself, would not kill, injure or do property damage, but indirectly may cause other things to happen that result in a hazard. For example, a major power or telephone service loss in a large city alone is not a direct hazard, but disruption to other critical services could create a variety of conditions that could directly threaten public safety.

The public’s perception of risk is an important factor to consider when crafting and disseminating information regarding hazardous situations. Alerting authorities should ensure that messages contain information that convey the true level of risk associated with a hazard, encourage taking protective actions, remain transparent, and avoid causing “alert fatigue,” while still erring on the side of public safety when dealing with conflicting or uncertain information about a threat.

Provide the Right Information

Alerting originators should work to understand how the public responds to messages. How individuals receive a message influences their perception of risk, which consequently impacts their timeliness in initiating protective actions. Provision of comprehensive, targeted, specific messaging enables the public to make informed decisions. This tactic limits milling; that is, people delaying taking protective actions after receiving a message to search for more information to help them decide what, if anything, to do. Messages should contain the following information: identification of the jurisdiction issuing the message (source); hazard type and impact consequences (hazard); the impact area boundaries (location);

protective actions to take, including when and how to take them and how taking them reduces impacts (guidance); and when the message expires and/or new information will be distributed (expiration time).

Furthermore, messages should be easy to understand, free of mistakes, and based on the most current information available. The alerting authority should coordinate with PIOs as soon as possible to ensure synchronized public-facing communications. Still, this coordination should not delay AWN issuances for rapid-onset incidents that may pose an imminent threat.

Account for the Public's Perception of Risk

Alert messages should be authoritative and confident. Still, alerting authorities must often issue messages under uncertain circumstances, as damages may be incurred before a threat can be verified. So to ensure the timely taking of protective actions, messages should be issued early, and message content geared toward the uncertainty of an incident (e.g., specifying an incident as "reported" and providing revised information as needed).

Additionally, people rarely act on a single message alone, so delivering messages through multiple channels increases public attention and audience reach, confirms message importance and authority, and encourages taking protective actions. Moreover, to gain recognition, AWNs should be issued from a trusted source.

Maintain Transparency

Messages should be transparent and honest. The alerting authority should not withhold information out of fear of causing panic, as this only serves to inspire distrust and forces people to seek information from other, less reliable sources. The alerting authority should also work to confirm hazardous situations, and policies should clearly identify what level of certainty is needed (e.g., confirmation from X independent sources, eyes on the scene) before issuing a message. Still, alerting authorities should use their best judgment but err on the side of public safety when deciding whether to issue an alert or warning that has the potential to turn out to be a false alarm or when dealing with conflicting or uncertain information about a threat. Incomplete or imperfect information is not a valid reason to delay or avoid issuing a warning. "When in doubt, warn."

Avoid Causing "Alert Fatigue"

Irrelevant messaging fatigues the public and causes recipients to discount or unsubscribe for further messages. As such, wide-reaching messages should be disseminated wisely and issued for imminent rapid onset; short detection to impact hazards that threaten life, health, public safety, security or property; and require immediate action, thereby maintaining future public receptiveness to alert messages for hazards that pose a significant threat.

Additionally, the alert originator needs to sort through a large amount of potential threat information (disseminated internally within a public safety entity for situational awareness) to determine each message's validity, the actual threat posed, and any follow-up actions to take or AWNs to issue to the public. Too many illegitimate or minor threat messages can cause internal "alert fatigue." To address this issue, the alerting authority should work to reduce the number of messages requiring an operator's attention, to prevent operators from overlooking hazards that pose a real or serious threat.

The following event codes are authorized by the SECB to all local jurisdictions with IPAWS capability.

Code	Definition
⚠ CDW	**Civil Danger Warning —** A warning of an event that presents a danger to a significant fraction of the civilian population. The CDW usually warns of a specific hazard and gives specific direction for protective action. Examples include contaminated water supply and imminent or in-progress terrorist attack. Public protective actions could include evacuation, shelter in place or other actions (such as boiling contaminated water or seeking medical treatment).
⚠ CEM	**Civil Emergency Message —** An emergency message regarding an in-progress or imminent significant threat(s) to public safety and/or property. The CEM hazard is less specific than the CDW. For example, the CEM could be used to for a 911 telephone outage or an emergency roadway detour.
⚠ EVI	**Immediate Evacuation —** A warning where immediate evacuation is recommended or ordered according to state law or local ordinance. As an example, authorized officials may recommend the evacuation of affected areas due to an event such as the release of a flammable or explosive gas. Authorized officials may recommend evacuation of designated areas where casualties or property damage from a vapor cloud explosion or fire may occur.
⚠ SPW	**Shelter in Place Warning —** A warning of an event where the public is encouraged 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). An example is the release of hazardous materials where toxic fumes or radioactivity may affect designated areas.
RWT	**Required Weekly Test —** A test message that consists, at a minimum, of the header and end-of-message tones. Though an RWT does not need an audio or graphic message announcing the test, RWTs are generally not relayed.

The following event codes are authorized by the SECB to certain state jurisdictions with IPAWS capability.

Code	Definition
 BLU	**Blue Alert** — An emergency message that rapidly disseminates information to law enforcement agencies throughout the United States to the media and the public about violent offenders who have killed, seriously injured, or pose an imminent threat to law enforcement, or when an officer is missing in connection with official duties. Blue Alerts provide details about the possible assailant(s), including physical descriptions, vehicle information and other identifying characteristics.
 CAE	**Child Abduction Emergency/AMBER Alert** — An emergency message, based on established criteria, about a missing child believed to have been abducted. A local or state law enforcement agency investigating the abduction will describe the missing child, provide a description of the suspect or vehicle and ask the public to notify the requesting agency if they have any information on the whereabouts of the child or suspect.
 NUW	**Nuclear Power Plant Warning —** A warning of an event at a nuclear power plant, classified as a Site Area Emergency or General Emergency as classified by the Nuclear Regulatory Commission (NRC). A Site Area Emergency is confined to the plant site; no off-site impact is expected. Typically, a General Emergency is confined to an area within a 10-mile radius of the plant.
RMT	**Required Monthly Test** — A test message that is generally originated by the state primary entry point (PEP) station, a state emergency management agency or by the National Weather Service and is then relayed by broadcast stations and cable channels. Monthly tests must be retransmitted within 60 minutes of receipt.

Hazard

In order to successfully send an IPAWS, 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.

Urgency	Severity	Certainty
Immediate Responsive action should be taken immediately	**Extreme** Extraordinary threat to life or property	**Observed** Determined to have occurred or to be ongoing
Expected Responsive action should be taken soon (within next hour)	**Severe** Significant threat to life or property	**Likely** Likely (more than 50% chance)
Future Responsive action should be taken in the near future	**Moderate** Possible threat to life or property	**Possible** Possible but not likely (less than 50% chance)
Past Responsive action is no longer required	**Minor** Minimal to no known threat to life or property	**Unlikely** Not expected to occur
Unknown Urgency unknown	**Unknown** Severity unknown	**Unknown** Certainty unknown

Messages are required by the CAP 1.2 standard 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.

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

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

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

Category	Description
Geo	Geospatial (including landslides)
Met	Meteorological (including floods)
Safety	General Emergency and Public Safety Security: law enforcement, military 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

Special Characters

When composing a message, avoid abbreviations. Because many devices are now text-to-speech (TTS) enabled, you should use only letters: (A-Z, a-z) and numbers (0-9).

Avoid the use of special characters (!, @, #, $, %, /, &, *, (,), _, +, -, =, ?, /, >, <, :, ;, {, }, [,], I), as they may not yield the result on screen you had expected.

Information Links and Telephone Numbers

Since SMS and IPAWS 90-character legacy messages are limited in length, including links in your message allows you to provide more detail and updates online. When adding a telephone number, remember to put a space between each number so that TT- enabled devices can read the number properly. If not, is could be confusing to the public.

To see how these characters interfere with the message or how the phone numbers or websites show up on message you are trying to send, try practicing with the IPAWS Lab during your monthly proficiency demonstration. See Section 3 for more details on the IPAWS Lab.

Spanish Language and Special Characters

You, as the alert originator, are responsible for your alert message content. Neither FEMA, nor wireless providers, nor consumer mobile devices will translate your English-language WEA message into another language for you. Please use an interpreter when possible to ensure accuracy in your messaging; you may have to reword your message due to the limitations of special characters. Just as in the English language, special characters are not allowed, so some adjustments may be required.

The alert language displayed on a phone is dependent on the phone type and settings on the phone. Some phones display both the English version of the alert and the Spanish version of the alert. Some phones may show only the English or Spanish version of the alert depending on the default language setting of the phone.

Tips for TTS messaging Category	Correct	Incorrect
Age	42 to 45 years old 42 years old	40-45 42 yrs old
Height	5 feet 6 inches 5 foot 6	5 ft 6 in
Speed	Miles per hour	Mph
Temperature	-30 degrees Fahrenheit	-30 degrees (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 (*must have a space)* 12 pounds	12lbs
Directions	North Northeast East Southeast South Southwest West Northwest	N NE E SE S SW W NW
License plate numbers	A B C 1 2 3 (must have a space between each character)	ABC123 ABC 123
Non-alphanumeric	Avoid special characters	
Addresses	1 4 2 2 5 1 4 2nd Street 5 0 6 2nd Street North 1 0 0 Ave. to 1 1 8 Ave. (requires period with Ave.) Use spaces between numbers. Be careful about dual-use abbreviations. St. = “Saint” rather than “Street.” “506 2nd St. N” becomes “Five Hundred and Six, second Saint N”. Minnesota Spell out words like Drive, Highway and State in full. Type out the full text to ensure proper pronunciation	14225 1 4 2nd Street 506 2nd Street N 100 Ave. to 118 Ave. (requires period with Ave.) Remember that numbers are spoken out in the tens and hundreds. So 12445 = twelve thousand four hundred forty five. MN
Telephone Numbers	7 8 0 – 9 8 0 – 8 7 5 8 9 1 1 Include spaces between each number.	780-980-8758 (Comes out seven hundred and eighty – nine hundred and eighty…) 911 (Comes out nine eleven)

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

Location

Alerting Options and Coverage Issues

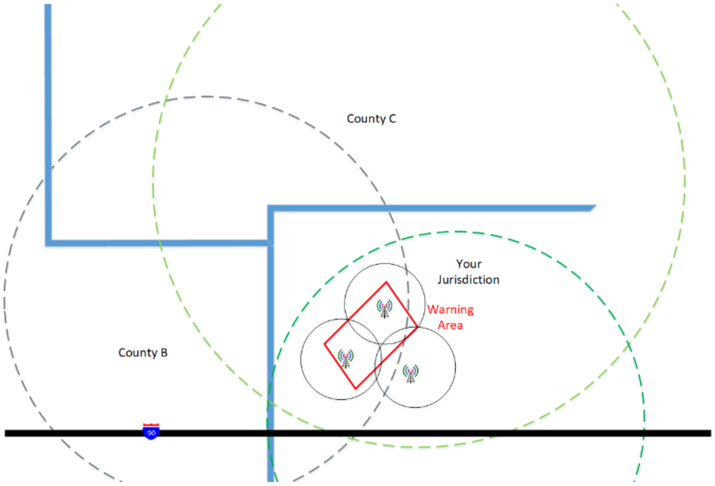
When preparing to send out alert messages, it is important to understand the potential coverage area of each alerting system. The following guidance shows how to incorporate each system into a layered approach starting from the system with the broadest reach to those that are capable of being scaled down to a small, geographically targeted area. In the tactics column, the colors mean the following: Green = Fastest – opt-out audience including visitors; Yellow = More direct opt-in audience; Red = Takes coordination; Gray = Warning limitations.

Tactic	Benefits	Barriers
WEA	- Targets a larger audience via cell phones. - Every mobile user with a WEA-capable device will receive an alert broadcast over WEA, unless they opt out. - Special needs communities tend to rely heavily on wireless devices. - Reaches tourists and visitors who are unlikely to have enrolled in a local service. - Avoids network congestion issues. - Grabs public attention, motivating receivers to seek additional information.	- Individuals can opt out, except for Presidential messages. - Cell coverage is irregular nationwide, especially in rural areas. - Definition of imminent threat is different nationwide. - Limited message length (90 – 360 characters). - Limit polygon to 100 point or FIPS/Code EAS.
EAS	- Reaches users listening to radio or watching TV. - Distinct noise grabs users' attention. - Verifies information from a trusted source.	- Users are trending away from cable TV and radio in favor of video streaming services. -Local; does not reach users on satellite TV. - Multiple alerts can lead to message fatigue. - Unable to target alerts with greater accuracy due to media markets.
Electronic Telephone Notification (ETN) **Mass Notification System** **Including opt-In cellular (voice)**	- Ability to target at-risk users through landlines in specific geographic areas through the use of specific groups. - Provides voice alerts for urgent incidents. - Easy to provide clear instructions on how to respond. - Ability to target at-risk users through cell phones in specific areas.	- Fragile infrastructure during natural disasters, which can also be costly; e.g., flooding. - Users are trending away from landline telephones in favor of mobile devices. - Once the user hangs up the phone, there is no way to access the alert or information. - Individuals tend to be suspicious of automated phone calls. - Accessibility issues if language barriers are not addressed. - Unlisted numbers, cell phones and numbers on "no-call" lists are not included on call databases unless manually added.

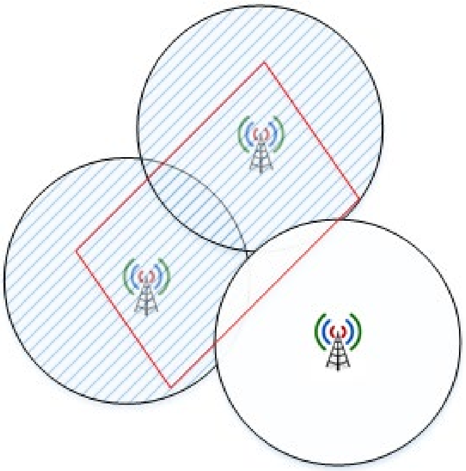
Tactic	Benefits	Barriers
Email opt-in	- Reach users on their computers and smart phones. - Ability for alert originators to send longer messages. - Easy to provide multimedia links, URLs or additional resources, when appropriate. - Users are able to filter the type of information they want to receive, allowing for more personalized alerts. - If the email is from an official source, it verifies information and builds trust.	- Requires users to sign up and opt in. - Requires personnel resources to educate users on availability and get them to opt in. - User(s) may not receive the email in timely manner. - Potential to lose a user's attention if the message has too much information.
Text/SMS opt-in	- Short-form messages are easy to send quickly. - If a text cannot get through, it keeps Trying. - Users can refer back to messages later. - Users are able to filter the type of information they want to receive, allowing for more personalized alerts (e.g., home address, work address, county). - Accessible for the hearing impaired and can use multiple language formats.	- Requires users to sign up and opt in. - Short messages are limited in effectiveness if they cannot grab a user's attention. - Space and character limitations may lead to confusion on actions to take. - A lack of sufficient information may result in a longer milling period (the time between receiving an alert and taking action). - Requires personnel resources to educate users on availability and get them to opt in. - Reaches users where they are, not where the warning is intended for.
Social media	- Usage is increasing nationwide, increasing potential reach. - Supports full alerts and warnings cycle, including preparedness and recovery. - Easy to push out information in real time. - Easy to provide multimedia links, URLs or additional resources when appropriate. - Can supplement traditional alerting tactics to provide more information, reducing milling periods. - Monitoring allows for more specific messaging, which can increase protective actions. - Easy to share information during non-emergencies to support public education on other alerting tools.	- User will only receive the alert if they are looking for information. - Misinformation is difficult to distinguish and combat. - Lack of credibility. - Depending on the platform, space for content can be limited or constricted by platform requirements. - Public expectation of a two-way dialogue may be unrealistic in times of imminent threat, resulting in issues. - Legal concerns. - Privacy concerns.

Tactic	Benefits	Barriers
National Oceanic and Atmospheric Administration (NOAA) Weather Radio All Hazards (NWR)	- NWR broadcasts official Weather Service warnings, watches, forecasts and other hazard information 24 hours a day, 7 days a week. - 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. - As of the publishing date of this best practice guide, no authorized Minnesota COGs can send an alert through the FEMA IPAWS OPEN system to the NWS system.
Traditional media (Press release, radio or tele-Vision broadcast, etc.)	- Easy to tailor content. - More detailed information. - More time to prep response. - Builds trust. - Emergency Management controls the information released and shared.	- Time consuming process, which sometimes results in information being out of date. - Information reaches the public slowly. - Public reach is limited. - Content tends to be no-nonsense, which feels less personal and engaging. - Media desire for breaking news can lead to errors or over-reach.
Website integration	- Can act as a home base for incident information. - Alert originators can update content. - Publicly accessible. - Allows for long-form, short-form and multimedia content. - Information comes from a verified source.	- Public is not automatically notified of updates. Users must seek out information. - Requires version control so users read the most up-to-date information. - Can be hard to find alert information on more complex websites, not easily accessible. - Requires coordination with IT personnel or a website provider.
Outdoor Warning Sirens	- Easily gets the attention of affected individuals in the area - Easy to educate communities on the meaning of a siren.	- Sirens may mean different things from community to community. - Limited ability to provide instructions for protective action. - Not effective with the deaf and hard-of-hearing.
Satellite radio and television	- Can reach the entire nation at once.	- Cannot be scaled down to a small area. - Only national alerts will be heard.
Route notification (e.g., knocking on doors)	- Information is directly from a trusted source. - Higher sense of urgency. - Reaches isolated communities.	- Time consuming and personnel intensive. - Reaches limited number of individuals. - Danger to the alert originator.

Coverage Areas



EAS and WEA Combined



WEA 1.0 and 2.0 Coverage

WEA 1.0

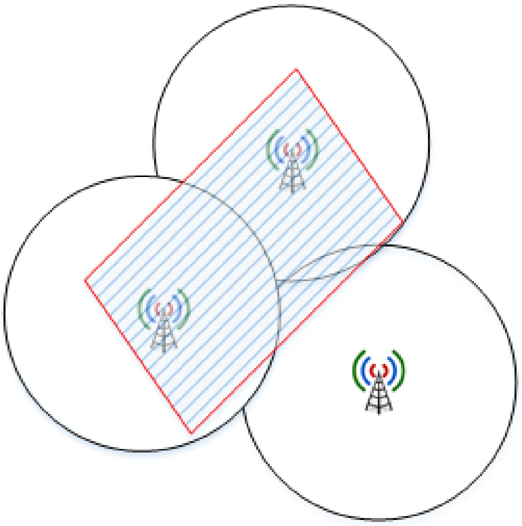
- 90 Characters

WEA 2.0

- 360 Characters English and Spanish and WEA Testing

WEA 3.0

- 1/10 of a mile overshoot outside the poylgon



WEA 3.0 Coverage

Geo-Targeting

Disseminating alerts based on recipients' location is important to ensure that those not at risk do not receive inapplicable messages. So, targeting should include people (and their devices) who are at risk from a hazard or who care about people and property at risk from a hazard, and alerts should be issued across areas where there is potential for the hazard to spread. If there is concern that people who are safe could think that they are unsafe, the warning message should address these individuals; for example, a message could state "people who live in other parts of the city will not experience flooding," and then also explain why these areas are safe.

Termination Time

The termination time is a requirement of the CAP 1.2 standard. It is designed to tell the broadcasting programs (WEA and other applications) when to stop broadcasting. Remember that you have up to 24 hours for a message to expire. When deciding on the termination time in WEA, consider these questions:

- How long does the message need to be out there?
- What's the danger?

Be aware that all applications do not react the same if you update or cancel an alert; see the table below.

Action	WEA	EAS
New Alert	New alert is created. Repetitive broadcast begins and continues through indicated lifespan of the alert.	New alert traverses the system and is broadcast at all broadcast points at one time (no repetition).
Update	Broadcast for the referenced alert ceases, and alert text is updated.	EAS treats it as new alert, so it traverses the system and is broadcast at all broadcast points at one time (no repetition).
Cancel	Broadcast for the referenced alert ceases.	No action taken if the alert has already been broadcast.

Agency Coordination

Alert messages that give false alarms or "cry wolf" may cause the public to become frustrated. Alert originators 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 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 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 event codes are automatically forwarded. Alerting authorities need to know which codes are automatically forwarded and w**hich 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 WEAs, the involvement of private sector partners in the wireless industry has expanded. Commercial mobile service providers (cellular carriers) partner with the FCC and FEMA. Due to this additional layer of dissemination and the variability of WEA implementation through the carriers, it is critical that PSAPs and emergency managers are aware of which cellular carriers operate in their jurisdictions and what WEA coverage may be available. Three of the major cellular carriers (ATT, T-Mobile/Sprint 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.

Coordination

When possible, communication about WEA messages 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.

Local media has a desire to keep their audiences informed of ongoing events. Besides their broadcast, 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 keys 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 communication of critical, time-sensitive information.

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

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 TTS. 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.

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.

Advantages of Templates for Standardizing Messages

There are a number of common elements 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 jurisdictions public information officer (PIO) to reduce coordination effort and time.

Use of Templates – WEA

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 1.2 standard)

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

- Urgency: immediate, expected, future, past, unknown
- Severity: extreme, severe, moderate, minor, unknown
- Certainty: observed, likely, possible, unlikely, unknown

Because WEA messages are limited to 360 characters (note that some may still only be capable of 90 characters; that why 90 characters is mandatory), 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 the recipient to other sources of information?
- If the message contains URLs or phone numbers, phone numbers must be spaced. For example 911 must look like 9 1 1 unless you want it to be a clickable resource, and some newer phones have TTS capability that may read it wrong without spaces.

It is recommend creating message templates not only for different scenarios but also for different communication channels, such as:

- WEA with a limit of 90 characters. This message is mandatory. .
- WEA with a limit of 360 characters. This is not a continuation of the 90 character message.
- Text messages, which have a limit of 160 characters.
- Twitter, which has a limit of 280 characters.

Some Examples

When defining the message template, you'll put the place holders in brackets and type the script as normal text. For example:

- **Morrison County Sheriff's Office: Water main break at** [location]. **Boil water until** [Expiration time]. **For updates,** [Info link].
    - You can even prompt for more specific information within the placeholders themselves:
- **Stevens County Emergency Management: Missing person** [name]. [Description including sex age ht wt hair]. **Last seen** [where] **wearing** [clothes]. **If seen,** [Guidance]. **For info,** [info link].

Although we suggest pre-defining scripts for specific types of emergencies, you can also make a very generic template by treating some of the script elements as tokens. For example:

- **Stearns County 911:** [Hazard] **at** [Location] **until** [Expiration time]. [Guidance][Expiration time].

Use of Templates – EAS

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:

- 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 TTS generation, if needed 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 TTS 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.

Some Examples:

- **CIVIL DANGER WARNING** Active shooter (CDW event code)
  This is an alert from [source]. An [hazard] active shooter is reported to be at/in [location(s)]. Please take safe cover immediately and as far away from [location(s)] as possible. [guidance] Call 9 1 1 from a safe location to report a shooter sighting. Do not call 9 1 1 for information. To repeat: [REPEAT MESSAGE]

- **SHELTER IN PLACE**: Chemical Spill or Fire (SPW event code)
  The [source] is responding to a chemical incident in [location]. Residents within a [number]-mile radius of [location] are advised to [guidance] shelter indoors immediately. If you are indoors, close and lock all windows, doors and vents, and turn off all heating and air conditioning units. If your children are at school in the affected area, they will be protected at the school. Do not travel to the school to get them. Do not call 9 1 1 unless you have an emergency to report. Do not call 9 1 1 for information. Tune to local radio or TV for updates on this situation and notification about when the shelter-in-place order will be lifted. To repeat: [REPEAT MESSAGE]

- **EVACUATION**: NATURAL GAS LEAK (EVI event code)
  This is an alert from [source]. There is a [hazard] natural gas leak in [location]. If you are in [location] or within [number] miles of this area, [guidance] evacuate the area immediately. If you are not in [location], avoid this area.

  To repeat: This is an alert from [source]. There is a [hazard] natural gas leak in [location]. If you are in [location] or within [number] miles of this area, [guidance] evacuate the area immediately. If you are not in [location], avoid this area. Tune to local radio or TV for important follow-up information.

Note: Due to EAS message time constraints, it may not be possible to include detailed information in the alert. Follow-up information should be provided to the media as quickly as possible.

Use of Social Media

Social media is the most critical method to instantaneously reach the greatest amount of people in an emergency, which makes it one of our most powerful alerting tools for both the media and public. Multiple social media platforms serve as a first source of information for people who want to know what is going on in their community.

Just as with the Electronic Telephone Notification system, the public must "follow" jurisdictions on various platforms receive these alerts. Social media is more successful when the community is engaged and aware of accounts prior to a disaster. Steadily interacting with the public during routine (non-emergency) operations builds trust with citizens so that they turn to public safety social media resources during an emergency or large-scale event. Engagement may include:

- Preparedness: Preparedness tips, humanizing stories, local community information.
- Response: Critical incident information, rumor control, live video updates.
- Recovery: Volunteer information, shelter locations, engaging photos of recovery efforts.

Social media also must stay current, or users will stop following posts. This includes communicating to audiences in a strategic and engaging manner using text, audio, images, graphics, maps and other data. Social media offers an opportunity for jurisdictions to engage with followers by answering questions. Monitoring comments and discussion groups is important during emergencies as people share personal experiences and individual impacts. Accomplishing these tasks may require additional staff and resources.

Social platforms currently used by the Minnesota Department of Public Safety (DPS) include:

- Facebook
- Instagram
- Nextdoor
- Pinterest
- Twitter
- YouTube

Here are some considerations for incorporating social media into alerts and warnings before, during and after emergencies:

- Social media outreach is highly dependent on working cellular and data networks that may be impaired or down during and following an emergency.
- Consider the variety of languages in your community and the complexity of the language in your post.
- Social media is highly effective at reaching the news media, which may assist in more broadly sharing messaging.
- Briefings and updates via live and recorded video are recommended when internet access and bandwidth allows.
- Allow public comments to be posted and seen; two-way engagement is expected by the public, and dedicated staff resources are necessary to facilitate it. This is controlled by rumor management personnel assigned to the Joint Information Center.

- Be aware that social media usage varies widely among different social, economic and demographic groups. Information gleaned from social media analysis may not reflect a balanced or complete picture.
- Ensure messaging is consistent across all alerting platforms.

Social media objectives should formally align to the jurisdiction's mission and strategy. The following are objectives to consider:

- What are you hoping to accomplish by using social media (e.g., engage in two-way conversation to address negative feedback, social media monitoring to dispel rumors)?
- Are your goals for non-emergency operations different than your goals for emergency operations?
- What are best practices and key lessons learned by partner agencies?
- How can your social media strategy support the achievement of larger jurisdiction objectives?
- Who else from your jurisdiction needs to be involved in the development of social media objectives (e.g., key decision makers, contacts from other departments)?
- What is the ideal tone for your social media presence (e.g., formal/informal)?
- How will your objectives determine the post frequency that makes sense for your organization?
- What is the content approval process, and who is part of the approval chain?

Benefits of Social Media

There are many benefits to social media that are not easily measured. Even so, they may greatly improve emergency management operations.

- Build trust with your audience and develop a reputation for your jurisdiction's vital resource.
- Amplify your agency's or partner agency's messages through shares.
- Enable your agency to crowdsource information for both planned and unplanned events.
- Combat misinformation and dispel rumors.
- Monitor and respond to both positive and constructive feedback.

If you are not using social media today but you want to start, focus only on those platforms that reach the most citizens and that are best-suited for distributing news. Follow these best practices as you begin building your jurisdiction's social media presence.

- Keep messages short and informative. Give citizens specifics, such as the location of emergency shelters or road closure updates.
- Link to more detailed content, such as emergency evacuation maps or shelter lists.
- Include hashtags to amplify the reach of your message (e.g., #Minneapolis).
- Send updates frequently, as citizens will expect continuous updates.
- Use an emergency mass notification system that integrates with your social media profiles to limit the number of times you need to draft and send the same message.
- Choose a mass notification system that integrates with IPAWS alert and warning channels (TVs, radios, wireless devices and NOAA weather radios).Continue to share updates even when an event has ended. Your citizens will still be interested in learning about recovery efforts.

Section 3: Administration, Training and Testing

Section Overview

This section introduces you to the skills required to effectively train for and maintain a strong alert, warning and notification program.

- Program Administration
- Training Requirements
- Memorandum of Agreement Process
- Establishing a Work Relationship with Your Software Vendor
- Training for New Hires
- Training, Practicing and Exercising
- IPAWS Training and Demonstration Environment
- Proficiency Demonstrations
- Live Code Testing
- WEA Testing (Background)

Program Administration

Documentation

- Signed memorandum of agreement (MOA) and DHS/FEMA Rules of Behavior
- Application for Public Alerting Authority (PAA)
- Copy of IS-247b. Introduction to IPAWS for each person who is authorized to send messages
- Warning software contract, service/help line information

Documentation

- Memorandum of agreement (MOA) / Rules of Behavior
- Public Alerting Authority (PAA)
- IS-247b. for each person who is authorized to send a message
- Warning software contract, service/help line information

Electronic Files

- IPAWS Digital Certificates in a secure location for both environments: Live and Test
- Copies of message templates created
- Master Street Address Guide (MSAG) Data download
- Map layers

Electronic Files

- IPAWS Digital Certificates for both environments: Live and Test
- Copies of message templates created
- MSAG Data download
- Map layers

Training Requirements

To ensure effective and efficient use of alert and warning capabilities, agencies must regularly train and exercise their alert and warning policies, procedures and systems. It is recommended that jurisdictions create a training program consisting of readily available coursework divided into sections of system access and responsibilities. The following is a recommended structure:

Alerting Originator – designed for those who can physically access and send on platforms within the jurisdiction's alert and warning program. FEMA requires the following course: IS-247b. Integrated Public Alert and Warning System (IPAWS) for Alert Originators.

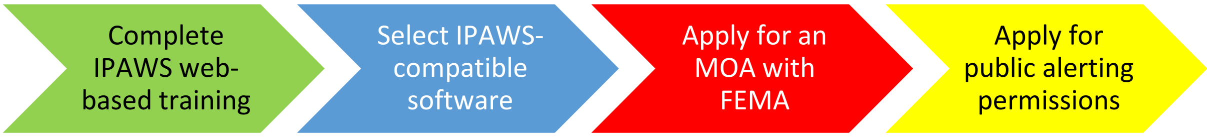
Alert Administrator – designed for those overseeing the entire alert, warning and notification program. FEMA requires all courses for the Alerting Originator level, and the person should be knowledgeable in cross-jurisdictional coordination techniques within the jurisdiction.

Recommended

- IS-29. Public Information Officer Awareness
- IS-251a. Integrated Public Alert and Warning System (IPAWS) for Alerting Administrators
- G-290. Basic Public Information Officer Course

Memorandum of Agreement Process

An active MOA must be in place between the FEMA IPAWS PMO and an alerting authority. The process for applying for IPAWS consists of the following four sections:



Complete IPAWS web-based training

Select IPAWS-compatible software

Apply for an MOA with FEMA

Apply for public alerting permissions

To apply, go to: https://www.fema.gov/integrated-public-alert-warning-system

Keep FEMA Updated on Changes to the MOA

An MOA is a business agreement between FEMA and an alerting authority. It is a written understanding of the Rules of Behavior regarding use of IPAWS and provides applicable agency information. It is imperative that all points of contact (POCs) mentioned in the MOA remain current in order to provide and receive pertinent IPAWS information. Maintaining current POCs is the responsibility of all parties.

Rules of Behavior

There are Rules of Behavior to consider when applying for an MOA with FEMA. These Rules of Behavior encompass the following:

- Using the IPAWS software for official purposes only, ensuring authorized users securely access the software.
- Ensuring authorized users have discrete and strong passwords for accessing the software.
- Ensuring computers hosting the software are protected and the software is used only from authorized devices.
- Ensuring authorized users agree to the software access agreement and understand that they are accountable for their actions in use of the software.
- Reporting security incidents to authorized personnel.

MOAs and digital certificate have a 3-year lifecycle. The digital certificate should be sent out approximately 10 days prior to expiring. If the alerting authority wishes to continue using IPAWS, the MOA must be renewed.

Digital Certificate

The IPAWS Program Management Office will reissue certificates as needed. The certificate should be added to the selected IPAWS-compatible software either by the vendor or user (dependent on software product). The certificate validates the identity of the issuing agency and serves to digitally sign the CAP message sent to IPAWS to ensure the message remains unchanged. The MOA and Digital Certificate have different expiration dates.

Changes to the MOA

Alerting administrators and/or agency personnel may decide to acquire different vendor software products when contracts expire or requirements change. It is important that Alerting Administrators keep the FEMA IPAWS PMO informed of software changes, in addition to changes to points of contact, address, etc. Please remember to notify the IPAWS office at ipaws@fema.dhs.gov.

Establishing a Working Relationship with Your Software Vendor

Establishing a working relationship with your vendor is the first step by asking about the following especially if you're not the one that was a part of the original contract process. Ask about their:

- Vendor-provided training.
- To clarify vendor-provided technical support.
- Exchange contact information.
- Look for 24/7/365 helpdesk availability.
- Trouble ticket process and response time.
- Software update notification.
- Participate in refresher trainings.

System Changes and Updates

Software products will always require updates. Alerting administrators need to be familiar with vendor processes for installation of new updates and changes to alerting software. Changes and updates may include: security and access control, user interface, added capabilities or features, and IPAWS updates.

Software Updates are Very Important

Are you notified when an update is being released? Are your updates automatically pushed, or does the vendor require the user to manually install update patches? It is important to familiarize yourself with your vendor's software update process. It is equally important to ensure your vendor has current contact information for you and your agency.

Prevent Unauthorized Access

Access control to IPAWS alert and warning software is extremely important. Alerting administrators should implement and employ applicable security protocols. Unauthorized access to IPAWS-capable software may result in errant alerts with serious repercussions.

Alerting administrators must:

- Develop security guidelines and Standard Operating Procedures (SOPs).
- Designate roles and responsibilities.
- Apply and reexamine user access controls (update when employees leave).
- Consider two-factor authentication.
- Require regular password change (e.g., every 90 days).
- Assign alerting privileges based on employee roles and responsibilities.
- Audit use of the system (who sent the alert).
- Stay current with vendor-provided security updates, if applicable.

Control Appropriate Level of Privileges for Employees

Alerting software providers should offer alerting administrators the ability to configure user permissions according to the following guidelines:

- Based on roles and responsibilities of personnel.
- Limited to personnel with ability to issue IPAWS alerts.
- Personnel can to perform administrative duties (e.g., view sent history and logs and run reports) without activating IPAWS.

Know When to Remove Someone's Access

Considerations with respect to removal of IPAWS permissions:

- Termination or resignation of employee.
- Changes in roles and assignments.
- Changes in plans, policies and procedures.

Training for New Hires

Alerting administrators should consider developing and enforcing internal training procedures and follow-up training. This training is critical for alert originators to remain proficient in sending alerts through IPAWS. Alerting administrators should also consider establishing new employee training procedures in addition to the regular IPAWS proficiency demonstrations completed through the IPAWS Training and Demonstration Environment, also known as the IPAWS Lab.

All training initiatives should include sending alerts and messages through IPAWS using the IPAWS Lab. Attention should be placed on understanding IPAWS permissions, software capabilities and functionality, and procedures specific to your agency.

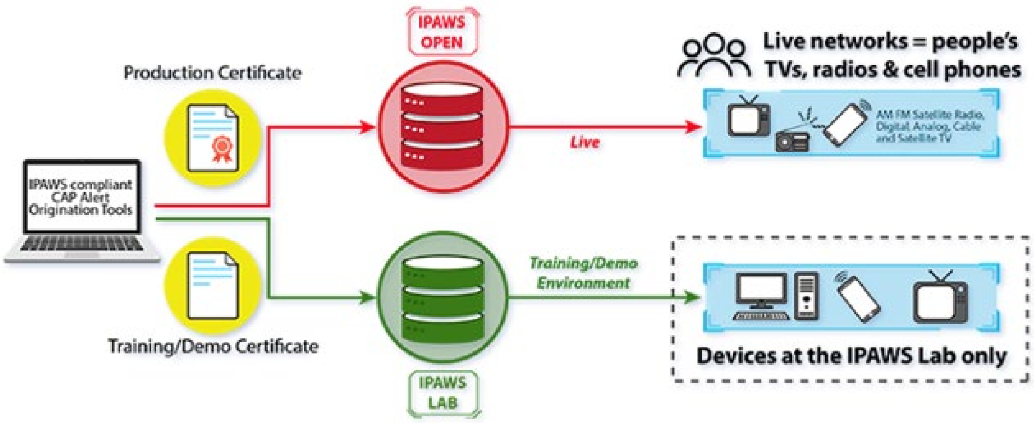
Training, Practicing and Exercising

Training, practicing and exercising your IPAWS alerting tools is a critical part of preparing to send effective alerts. Benefits include: Understanding capabilities and functionalities; evaluating software tools with respect to agency requirements; assessing staff progress and familiarization with software tool; and identifying gaps in plans, policies, and procedures

The IPAWS PMO provides public safety officials with a controlled IPAWS environment where alert and warning technologies can be exercised to assess capabilities and effectiveness with IPAWS.

The IPAWS Lab is a closed IPAWS environment capable of demonstrating alert dissemination to all IPAWS pathways, including the EAS, WEA, Non-Weather Emergency Messages (NWEM), and internet-based technologies.

The primary purpose of the IPAWS Lab is for public safety officials to gain confidence and build proficiency by using IPAWS in a safe and closed environment. Other purposes of the IPAWS Lab include alert and warning functional assessments, alert dissemination validation, training, exercises, procedural and process evaluation, and the establishment of functional requirements.


IPAWS OPEN
Production Certificate
Live networks = people's TVs, radios & cell phones
AM FM Satellite Radio, Digital Analog, Cable and Satellite TV
Live
IPAWS compliant CAP Alert Origination Tools
Training/Demo Environment
Training/Demo Certificate
Devices at the IPAWS Lab only
IPAWS LAB

IPAWS Training and Demonstration Environment

Virtual Use

One method available to participants is virtual access to the IPAWS Lab. The virtual method allows participants to attend a webinar with IPAWS Lab personnel. Benefits include:

- Virtual hands-on; attendee shares screen.
- Practicing procedures.
- Observing/discussing scenarios.
- Building templates based on hazards.
- Practicing activation of EAS and WEA.
- Observing alert dissemination.
- Using lab equipment to demonstrate alert origination and dissemination.

Message Viewer Use

Another way to access the IPAWS Lab is via the IPAWS Message Viewer. Advantages for this type of IPAWS Lab use include:

- User-friendly web interface.
- Alert dissemination verification.
- Viewing status/error codes.

- Troubleshooting, if necessary.
- 24/7 availability.
- No need to schedule time with Lab personnel.
- Alerts available for review on IPAWS Message Viewer for 24 hours.

Training Frequency Recommendations

Alerting administrators should require personnel to conduct regular training, practicing and exercising as it relates to their agency's IPAWS plans, policies, and procedures.

FEMA recommends that alerting administrators seek software vendors that provide regular refresher training on new features and functions of their software. Web, computer, and/or video training should be available to users as a regular refresher on the processes and procedures of using the software. This should be given by the software vendor at least annually.

You can contact the IPAWS Lab 24/7: 1-84-IPAWSLAB / **1-844-729-7522**

Proficiency Demonstrations

Alerting administrators play a critical role in the success of the implementation of national policy for the protection of life and property. It is imperative that public confidence in our alert and warning systems remain high and the information provided to the public be clear, authoritative and trusted.

For this reason, alerting administrators must ensure their COG demonstrates the ability to compose and send a message through the IPAWS system at regular intervals. Such demonstrations must be performed on a monthly basis by generating a message and successfully sending it through the IPAWS Lab.

Guidance from FEMA for a Successful Proficiency Demonstration

The below guidance applies to sending a successful controlled test message via a COG alert originating software to the IPAWS Lab Cloud Environment.

- Submit a successful message to the IPAWS-OPEN Lab Cloud Environment using your COG assigned training/demo certificate at least once a month.
- COGs can conduct their proficiency demonstration at their own discretion.
- The proficiency demonstration can be conducted at any date/time within the given month.
- The message must be for EAS and/or WEA, depending on your COG's approved alerting permissions. If a COG is approved for both channels (EAS/WEA), then both channels must be tested simultaneously if the software provides the capability.
- The proficiency demonstration message (EAS description/WEA 90-character message text) shall be as follows: **"TEST TEST TEST. This is a Proficiency Demonstration Test Message. No action is required."**
- COGs may use any approved event code for the test message. Neither additional message content nor use of a geo-targeting polygon will be evaluated.
- The IPAWS Message Viewer can provide alert originators with confirmation of whether the test message was successful: **(30xxxx= replace xxxx with your COG ID)**: https://ipawsopen-lab.net/ALERT_SERVICES/postedmessages.php?COGID=30xxxx
- Successful message codes are 500 for EAS and 600 for WEA.

- Further details on the IPAWS message viewer are available at: https://www.fema.gov/media-library/assets/documents/106754

Live messages sent to the production environment will not be counted as a Monthly Proficiency Demonstration.

Minnesota Guidance for a Successful Proficiency Demonstration

The alert originator has the ability to log in and:

- Identify the digital certificate expiration date.
- Verify user connectivity to IPAWS.
- Start by sending an RWT to ensure it is connected to the correct location.
- Create a new message using the following criteria:
  - Choose proper event code.
  - Create a polygon or circle of less than 10 polygons (some vendors don't support this) or 100 nodes.
  - Create free-form 90 and 360 character WEA text while avoiding prohibited characters.
- Send an alert to multiple channels (WEA, EAS, NWEM, etc.).
- Select a pre-populated template and fill in to the greatest extent possible.
- Update or cancel an alert without having to reenter all the data.

The alert administrator has the ability to:

- Check an alert message template for errors prior to sending.
- Review alert history and/or logs for possible errors.
- Define IPAWS alert status codes for sent alert, with a determination what the advice codes means.
- Engage vendor support to include user training and around-the-clock technical support.
- Create user ID and passwords based on the provided guidelines.

Live Code Testing

If either EAS or WEA options are selected to be used in a live exercise, public outreach campaign, etc., you must first ask yourself of the benefits and barriers to each. Live code testing is not taken lightly; it requires some thought about why, what data are you going to collect, how you're going to report it, and to whom. With that, the following considerations need to be given to both EAS and WEA.

EAS

EAS Does not require an FCC waiver, but requires you to coordinate with the SECB IPAWS Committee with a recommended four months' advance notice. Put the notice in writing and include what you intend to accomplish with the message, how you intend to collect feedback from the public, and a detailed after-action review (AAR) to the SECB IPAWS committee for review. See information below for more details.

WEA

The FCC waiver requires a recommended four months' advance notice. Put the notice in writing and include what you intend to accomplish, how you intend to collect feedback and data from the public, and a detailed AAR to the FCC for review. The following information will give you more details.

Requesting a Waiver for a LIVE CODE Test

FCC rules are detailed in 47 CFR Part 11; guidance on Tests of EAS Procedures (Section 11.61) and Prohibition of False EAS Transmissions (Section 11.45) is provided. The FCC states these rules are designed to prevent public misunderstanding or, far worse, public panic in connection with EAS activations that do not signal the onset of an actual emergency.

State and local emergency authorities in many areas have concluded that they require use of "live" or real event codes for certain tests.

The Public Safety and Homeland Security Bureau of the FCC emphasizes that organizations seeking to do a test using live event codes must describe fully the steps they will take to mitigate risk. Such steps shall be coordinated with the Minnesota SECB IPAWS EAS work group to ensure the public, media, PSAPS, and other members of the first responder community are fully aware of the tests and, specifically, that live event codes will be employed.

The following guidelines could help minimize the potential for falsely alarming the intended or unintended audience:

- Conduct EAS/WEA tests using real event codes no more than once or twice annually.
- Conduct EAS/WEA tests using real event codes in lieu of the Required Monthly Test (RMT)/Required Weekly Test (RWT) on the typical date and time when possible.
- Conduct the EAS/WEA test using a real event code when the hazard is not expected. Have a contingency plan that includes postponing the test to a later date in case hazardous weather is forecast for or unexpectedly develops on the test date..
- Conduct an extensive public awareness campaign (including outreach and education) that intensifies in the weeks and days leading up to the test.
- In this campaign, use multimedia Public Service Announcements (PSAs):
  - Use news releases.
  - Provide interviews.
  - Post announcements to email list servers.
  - Highlight the test on webpages, social media, etc.

- Prior to the test, issue one or more public statements explaining why and when the test will be conducted and provide a website where the intended audience can provide feedback.
- Make potentially affected institutions, agencies and organizations, such as school systems and international partner agencies (i.e. test occurs in a state along an international border), aware of the test.
- Define the "intended audience" that could potentially be falsely alarmed by the EAS test using real Event Codes and, as well as possible, identify all potential "receiver methods" within that intended audience. The most common receivers are TVs, radios and NWR receivers. Other

receiver methods could include websites, cell phones, programmable highway signs, in-vehicle navigation, etc.

- Take mitigation measures, to the extent possible, against the automated receiver methods identified above that will not carry the complete text of the test message, to eliminate or minimize the potential of falsely alarming the audience.
- Ensure the test message will expire shortly (e.g., typically 15 minutes) after it was issued. This will remove the test message as quickly as possible from most automated displays that would not be mitigated.
- Ensure the actual text of the test message is determined and coordinated by the Minnesota IPAWS EAS work group well in advance of the test date. The text should emphatically state this is indeed a test, explain briefly why the test is taking place, and provide a website where the intended audience can provide feedback.
- Immediately after the test message expires and for no less than two hours, issue at least one public statement stating the test is completed, why it took place and provide the web site for the intended audience to provide feedback.
- Collect key findings from the test:
  - Did you receive the test message?
  - How did you receive the test message?
  - What is your ZIP code, etc.?
  - Phone information:
    - Phone manufacturer.
    - Model.
    - Operating system.
    - Are you in the targeted area? If not, how far outside of the target area are you?

- Report results through an AAR copy furnished to the SECB IPAWS Committee.

Obtaining a Rule Waiver

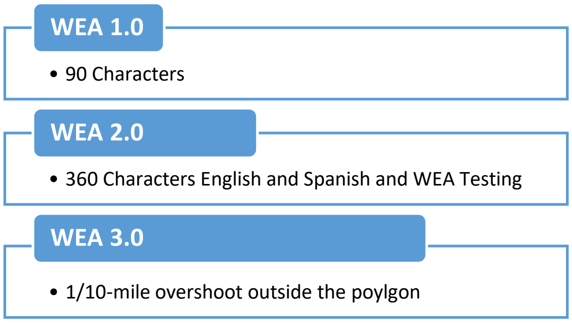
1. Consult with the Minnesota IPAWS Committee well in advance of conducting an EAS/WEA test (four months).
2. Give a detailed proposal to the Minnesota IPAWS Committee that includes a letter to send to the FCC and details on how you will do the test (include information such as websites, who you will contact, how you will notify the public etc.).
3. The Minnesota IPAWS Committee will work with you on making sure all the requirements are met and forwarded to the FCC.
4. The Minnesota IPAWS Committee will notify the requesting agency when the request is approved or denied.

For any questions about EAS or WEA testing, email us at ecn@state.mn.us.

WEA Testing (Background)

State/local WEA tests are a new category that perform like any other WEA alert, with the exception that only wireless subscribers that opt in will receive them. No waiver is required.

- Allows for live test of WEA.
- FCC waiver not needed for RMT.
- Public outreach not necessary.
- Not all software vendors are WEA 2.0 and 3.0 compatible.
- Urgency-Severity-Certainty Requirement.
- Not all phones support state/local testing.
- Not all phones support WEA 2.0 and 3.0 capability.
- **Does not meet monthly FEMA proficiency demonstration requirement**.



WEA 1.0

- 90 Characters

WEA 2.0

- 360 Characters English and Spanish and WEA Testing

WEA 3.0

- 1/10-mile overshoot outside the poylgon

Before you begin WEA testing, give some thought to the following:

- Purpose and methodology: What are you going to accomplish, and how are you going to go about it?
- Expectations: What do you want the end state to be?
- Monitoring:
  - Include different phone manufactures and wireless providers.
  - Determine locations in your jurisdiction to target.
  - Data collection: What data are you going to collect at a minimum?
    - Phone manufacturer.
    - Model.
    - Operating system.
    - Whether user is in target area or how far outside target area.
- Report results through an AAR copy furnished to the SECB IPAWS Committee.

Before you begin, pre-test using the IPAWS lab, gain confidence and expertise.

Recommended message text

90 character: This message is mandatory. Note that the 360-character message is not a continuation of the 90-character message.

***"This is a test of the wireless emergency alert system. No action required.* [your jurisdiction]"**

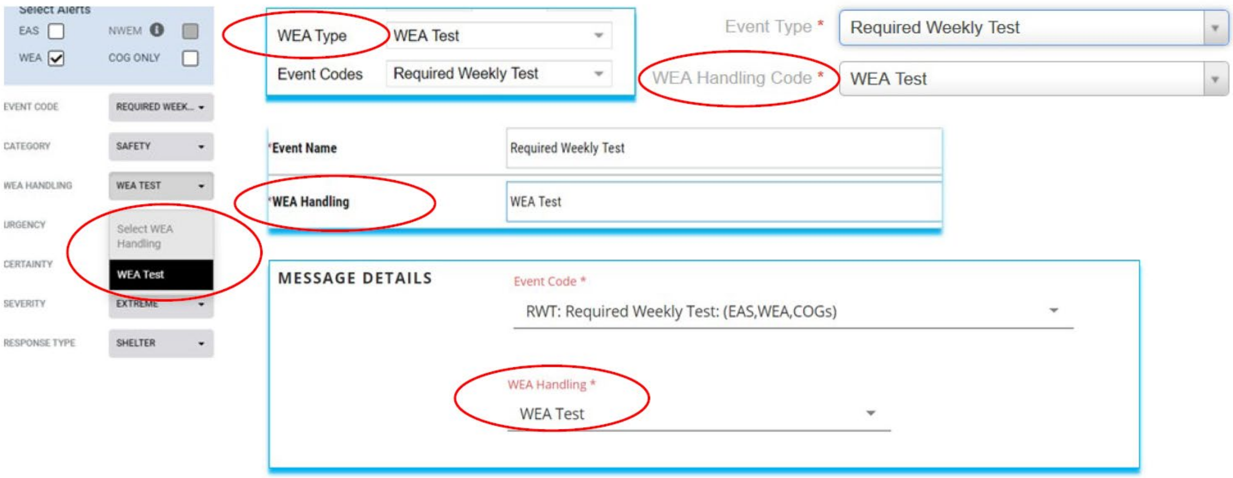
The message is 75 characters long, leaving space for your abbreviated jurisdiction name.

360 character:

"This is a test of the wireless emergency alert system. This test is being performed by [your jurisdiction name]. No action required. Go to [insert URL, for the web site, survey etc.] for additional information or call [insert number]."

Insert your jurisdiction’s URL or a link to a survey page you want them to fill out upon receipt of the message. You can also test the click ability of a phone number.

No matter what software platform you’re using, you have to use a 90-character message as a starting point, and then a 360-character message. Although the 90- and 360-character Spanish messages are optional, they are highly recommended for those jurisdictions with a large Spanish-speaking population.



Select Alerts

EAS □ NWEM ■ COG ONLY □

WEA ☑

EVENT CODE: REQUIRED WEEK...

CATEGORY: SAFETY

WEA HANDLING: WEA TEST

URGENCY: Select WEA Handling / WEA Test

CERTAINTY

SEVERITY: EXTREME

RESPONSE TYPE: SHELTER

WEA Type: WEA Test

Event Codes: Required Weekly Test

Event Type *: Required Weekly Test

WEA Handling Code *: WEA Test

*Event Name: Required Weekly Test

*WEA Handling: WEA Test

MESSAGE DETAILS

Event Code *: RWT: Required Weekly Test: (EAS,WEA,COGs)

WEA Handling *: WEA Test

Remember to use the **WEA Handling code**: **WEA Test** and RWT to test.

Try a few scenarios in the **test environment** first to see how it goes. Some examples are: Draw a polygon;

- Around small town in your jurisdiction.
- Around part of a large city in your jurisdiction.
- Over your jurisdiction border into the next county.

If all three of the above work, move on to testing in the **live environment**.

Above all, when testing, let the PSAP in the neighboring county know ahead of time, epically when testing near or over their border.

Viewing Live Alerts

To view a live WEA alert or test in real time, go to: http://warn.pbs.org.

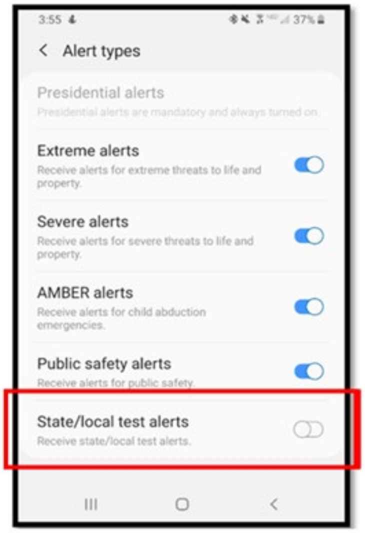
Setting Up Cell Phones to Receive Tests

Most WEA-capable phones can now receive a new WEA alert class: WEA test. Recent models of Android and Apple iOS phones and those upgraded to newer operating systems will have this setting available. However, these phones ordinarily ship to the customer with the WEA test setting disabled. The user must take specific action to enable it to receive test alerts.

Note: To receive a WEA test, Wi-Fi has to be off or not connected. If it is, you may not receive the test.

Android OS

In Android phones, the exact location of the options to enable WEAs varies. We recommend that you use the search function in the Settings app to find *Emergency Alerts*. Turn on *State/local test alerts or* a similar setting you may see, if it is available on your phone.



Presidential alerts
Presidential alerts are mandatory and always turned on.

Extreme alerts
Receive alerts for extreme threats to life and property.

Severe alerts
Receive alerts for severe threats to life and property.

AMBER alerts
Receive alerts for child abduction emergencies.

Public safety alerts
Receive alerts for public safety.

State/local test alerts
Receive state/local test alerts.

In this Android example, public safety alerts are automatically opted in.

WEA test appears here as “State/local test alerts” and is automatically opted out, but the user can switch it to opt in.

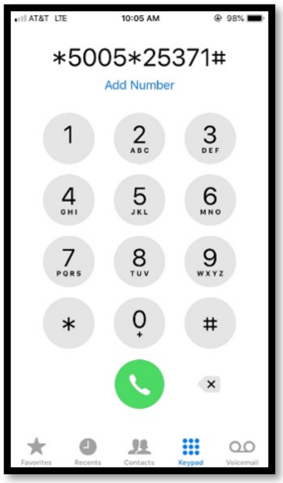
Newer and upgraded phones will have WEA test capability.

Apple iOS

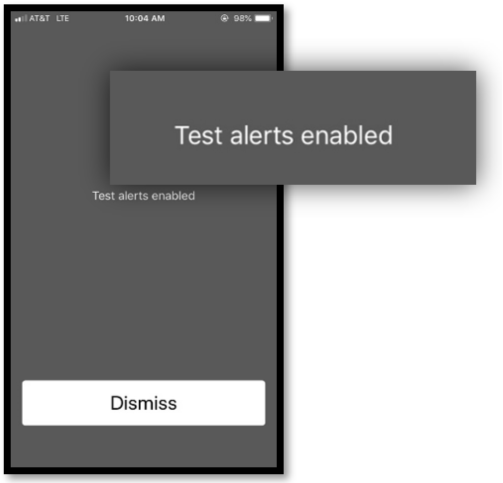
When your iPhone is connected to a carrier in the U.S. — using a U.S. SIM card or while roaming in the U.S. — you can enable test emergency alerts. By default, this is turned off. When you receive this type of alert, you'll hear a sound that's similar to an alarm, and the alert will mention that it's a test. To turn these alerts on or off, follow these steps:

Open the Phone App and tap Keypad.

To opt into test emergency alerts: Enter *5005*25371# and tap☎. You’ll get an alert that says “Test alerts enabled.”



*5005*25371#



Test alerts enabled

Test alerts enabled

To opt out of test emergency alerts: Enter *5005*25370# and tap☎. You’ll get an alert that says “Test alerts disabled.”

Acronym List

Acronym	Meaning
AMBER Alert	America’s Missing Broadcast Emergency Response
CAP	Common Alerting Protocol
CMAS	Commercial Mobile Alert System
CMSP	Commercial Mobile Service Providers
COG	Collaborative Operating Group
EAS	Emergency Alert System
EMI	Emergency Management Institute
EDXL-DE	Emergency Data Exchange Language - Distribution Element
FCC	Federal Communications Commission
FIPS Codes	Federal Information Processing Standards Codes
HazCollect System	National Weather Service All-Hazards Emergency Message Collection
IPAWS	Integrated Public Alert and Warning System
IPAWS-OPEN	IPAWS Open Platform for Emergency Networks
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NWEM	Non-Weather Emergency Message
NWR	National Weather Radio
NWS	National Weather Service
OASIS	Organization for the Advancement of Structured Information Standards
PEP	Primary Entry Point Stations

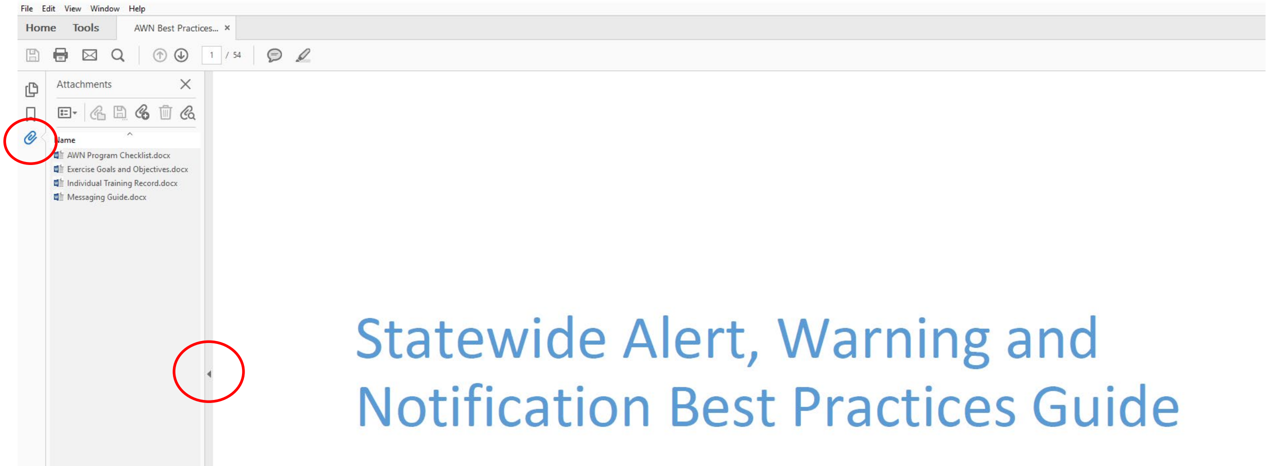
PMO	Program Management Office
SOP	Standard Operating Procedures
WEA	Wireless Emergency Alert

A glossary of alert and warning terms can be found at www.fema.gov/informational-materials

NWS EAS codes can be found here: https://www.weather.gov/NWR/eventcodes

Bonus Material

Additional check list and table excerpts are attached to the document is word format so they can be tailored and printed for use locally. You can access them by clicking on left margin then click on paper clip icon in the left margin to access the attachments.


File
Edit
View
Window
Help
Home
Tools
AWN Best Practices...
1
/ 54
Attachments
Name
AWN Program Checklist.docx
Exercise Goals and Objectives.docx
Individual Training Record.docx
Messaging Guide.docx
Statewide Alert, Warning and Notification Best Practices Guide

File name	Description
AWN Program Checklist.docx	A form used to check off pertinent records and files you should have on hand for alert and warning.
Evaluation Goals and Objectives.docx	Evaluation guidance for a messaging exercise with objectives to see a message go out and where and how it is received.
Individual Training Record.docx	Track an employee's level of training and FEMA Proficiency Demonstration(s)
Messaging Guide.docx	A quick reference guide for sending out a message to the public.
Public Information and Warning EEG Template 2020 508.docx	An Exercise and Evaluation Guide for messaging.