Alerts, Warnings, and Notifications Guide

November 2024

Table of Contents

This document was prepared for the state of Idaho Office of Emergency Management by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), Interoperable Communications Technical Assistance Program (ICTAP) as part of Work Order #WO23-290. Additional information about the program can be found at: https://www.dhs.gov/safecom/ictapscip-resources.

Any use of a manufacturer's name in this report or the discussions that were conducted does not constitute an endorsement of any manufacturer or their products by CISA.

QUICK REFERENCE; HOW TO ALERT THE PUBLIC

STEP	ACTION	✓
ON-GOING PROGRAMMATIC ITEMS		
1	Review this guide which will describe the program and necessary steps.	
2	Contact IOEM for further procedural guidance on becoming an alert authority in Idaho.	
3	Follow the procedure in Appendix B and become an alert authority recognized by FEMA and authorized to use the Integrated Public Alert and Warning System (IPAWS) IPAWS is not the only method to alert the public but it is the most complete and time efficient. As part of this application process your agency will need to select one of the service providers listed in Appendix D.	
4	If not already established, develop a long-term public alerting standard operating procedure (SOP) for your local entity and share that with neighboring jurisdictions.	
5	Maintain alert origination and authority status on a monthly recurring basis thru proficiency demonstration so that you are ready.	
GENERATING AN ALERT		
1	Craft and format your message IAW FEMA guidelines and alerting software constraints.	
2	Determine avenues for dissemination (broadcast, cellular, social media, etc. or ALL).	
3	Determine your intended audience and what information you desire the public to act on.	
4	Issue the alert and supplementary messages as necessary to facilitate action during and after disaster response actions.	
5	If you are not an alert authority and do NOT have a previous agreement with a neighboring jurisdiction you may choose to contact the State Communications Center (STATECOM) to assist in issuing an alert for you.	

Introduction

Welcome to the first consolidated Alerts, Warnings, and Notifications (AWN) Guide developed to support the people of the State of Idaho. Public alerting is a critical component in both effective emergency management and managing efforts to protect our citizens. History has taught states across our nation that alerting, warning, and notifying the public before, during, and after disasters leads directly to saving lives, protecting property, and setting the conditions for a more efficient response and recovery.

This guide was developed in robust collaboration with our federal, state, local, and tribal partners. It strives to provide a comprehensive, yet easy to understand guide for stakeholders across the public safety and emergency management landscape. It was created to help ensure that the citizens and visitors to Idaho are notified of life-threatening situations in as timely and accurate manner as possible.

The guide is designed as a companion to the already published and recognized Idaho Emergency Alert System (EAS) State Plan developed and approved by the State Emergency Communications Committee (SECC). Likewise, this AWN guide has been reviewed and endorsed by the Idaho Public Safety Communications Committee (IPSCC), and Idaho's six regional District Interoperability Governance Boards (DIGBs). All three of these governance entities are dedicated to providing on-going, continuous improvement to public alerting methods and procedures across the state.

Through this resource, local, state, and tribal officials will gain a clear understanding of the public alerting process, including the systems that support effective messaging and how to manage them to achieve maximum efficiency and minimize confusion. This in turn, will enhance preparedness, response, and recovery efforts while keeping the public informed, saving lives, and protecting property and the environment.

Document Revision Process

The Idaho Alerts, Warnings, and Notifications Guide is reviewed, at minimum, every two years. The Idaho Office of Emergency Management (IOEM) Emergency Communications Program Manager is responsible for conducting the review. Time-critical updates may be initiated and submitted at any time using this same process. Any updates or changes to this document will be submitted to the SWIC for approval prior to implementation.

Once approved, all changes to the document are recorded in the Revision Record.

Revision Record

VERSION	DATE	DESCRIPTION OF CHANGE
1	07/17/2024	Original document creation

1. What are Public Alerts, Warnings, and Notifications?

A **public alert** is a communication intended to alert the public and direct their attention to an immediate occurring risk or hazard. Public alerts may also include instructions for potential protective actions and provide ongoing communications relevant to an event.

A **public warning** is a communication intended to notify the public of an imminent event and to persuade them to take one or more protective actions to reduce losses or harm.

Notifications include public and internal notifications. These notifications/advisories are not to be used for promoting public or private events. Public notifications/advisories can include protective actions, evacuation routes, boil water advisories, traffic advisories, and return from evacuation notices, while internal notifications/advisories provide communications and information as defined by the agency.

In all cases, alerts, warnings, and notifications should be reserved for situations which could endanger the public and/or cause serious property/environmental damage. Use of public alerting tools and software are not to be taken lightly and should never be leveraged for political, marketing, or trivial messaging.

1.1 Timeframes for Issuing Alerts and Warnings

Agencies should always have an alerting capability ready, with both primary and backup systems in place. Being able to send out alerts is crucial for informing the public quickly in case of emergencies. Agencies should promptly issue alert and warning messages, with staff having quick access to alerting systems and proper training. Limited resources and non-operational equipment should not delay the alerting process. Table 1 below provides the timeframe for alerts, warnings, and notifications issuance.

Table 1: Alerts, Warnings, and Notifications Timeframe

Type	Timeframe	Purpose	Examples
Alerts	At the beginning of and during incidents with an ongoing, immediate threat	Accesses the public by drawing their attention to risks or hazards	Active shooter and other civil dangers, hazardous materials concerns, 911 outage, America's Missing: Broadcast Emergency Response (AMBER) alerts
Warnings	Prior to incidents	Distributes guidance to prepare for an anticipated incident	Weather watches/warnings, fire warnings, volcano warnings, evacuation orders
Notifications	During and after immediate threats, also includes non-event related messaging	Instructs immediate protective actions and provides ongoing communications relevant to an event and conveying time sensitive information on response and recovery related services	Protective actions, evacuation routes, boil water advisories, return from evacuation notices, area accessibility updates, all- clear notices

2. Roles and Responsibilities

Multiple levels of government are responsible for planning, preparing, and disseminating alerts and warnings. Each level of government—and designated entities within those levels—holds responsibility and/or authority to ensure the overall effectiveness of the statewide alerts and warnings system in the state of Idaho. A primary responsibility of the state is to facilitate the implementation of the Integrated Public Alert and Warning System (IPAWS) and other emergency notifications into the emergency notification network. In the case of a catastrophic local, state, or regionally defined event, the state must provide a resilient and comprehensive alert and notification capability.

It is recognized that some agencies have procured alerts, warnings, and notifications software that may or may not interface with the IPAWS system. Agencies that have IPAWS origination capabilities should follow the procedures set forth by this guide and by the Federal Emergency Management Agency (FEMA) IPAWS program. Those agencies that do not have IPAWS origination capabilities within their software should still strive to utilize best practices for alerts, warnings, and notifications.

2.1 Key Individual Roles

Roles and responsibilities of alerting differ amongst agencies; however, it is important to understand the key individual roles that exist in the alerting ecosystem.

- An **Alerting Authority** is a jurisdiction with the designated authority to alert and warn the public. An approved Alerting Authority can access IPAWS through a unique, individually identified account so that every warning message is attributable to a specific individual. Using shared agency accounts to control access to warning systems can undermine the enforceability of usage policies and is not allowed. All IPAWS users should utilize a strong password for authentication. Ensuring the security of the system will reduce the chance of data breaches and ensure the public's trust in providing their contact information to an opt-in system.
- **Alert Originators** are the individuals assigned to originate an IPAWS alert using Common Alerting Protocol (CAP)-capable software. This position utilizes IPAWS in accordance with agency plans, policies, and procedures while also developing and/or providing input to Standard Operating Procedures (SOPs) and other instructional materials.
- An **Alerting Administrator** is the authority responsible for implementation and use of IPAWS in accordance with agency policies, plans, and procedures.
- In Idaho, the **State IPAWS Administrator** is co-served by two individuals: the IOEM Emergency Communications Program Manager serves as the primary IPAWS Administrator, and the Statewide Interoperability Coordinator (SWIC) serves as the alternate and back up administrator. The roles of the state IPAWS administrator include educational outreach on public alerting topics, primary interaction with FEMA regarding IPAWS, review and administration of Memorandum of Agreements (MOAs) and Public Alerting Applications (PAA), and ongoing status coordination with Alerting Authorities across Idaho.

2.2 Local and Tribal Alerting

Local and tribal officials have a responsibility to keep the public informed about natural, human-caused, and technological disasters, and to provide guidance regarding what protective actions the public needs to take. Examples of actions that the local officials can provide to the public include but are not limited to:

- Evacuation information including evacuation routes, shelter info, key information, etc.
- Locations of points of distribution for food, water, medicine, etc.
- Hazardous materials incidents information
- Lockdown
- Shelter-in-place guidance
- Health advisories
- 911 outage

Specifically, jurisdictions that are IPAWS-qualified should consider:

- Enacting ordinances and/or policies identifying local roles and responsibilities to enable the issuance and coordinated dissemination of alerts and warnings to the public by responsible officials within their jurisdictions regarding imminent threats to human life and health and serious threats to property.
- Training users and installing, maintaining, and exercising/testing local public alert and warning capabilities within their jurisdiction.
- Understanding the access and functional needs-related considerations associated with public alerts and warnings systems and messaging.

- Optionally obtaining authority and tools for accessing federal warning systems as a Collaborative Operating Group (COG) via the FEMA IPAWS, if so desired.
- Participating in revisions of mandated Federal Communications Commission (FCC) local EAS plans, including approval of authorized event codes.
- Developing procedures for proper chain of command for initiating, cancelling, and revoking accidental alerts, and for rapidly correcting and updating alert details as additional information becomes available.
- Non-Weather Emergency Messages (NWEM): Coordinating with adjoining jurisdictions, operational areas, the state, and the National Oceanic and Atmospheric Administration (NOAA) National Weather Service (NWS) regarding origination of alerts and warnings over NOAA Weather Radio related to hazards that have effects across jurisdictional boundaries.
- Participating in required monthly proficiency IPAWS tests as directed by the FEMA IPAWS office.
- Developing a policy outlining the authorized personnel who may act as backup and transmit alerts on behalf of the affected entity in the event of system failure.

Many agencies have multiple notification/alerting systems that can deliver both emergency and non-emergency information to their communities. These systems include but are not limited to opt-in notification methods similar to the Idaho State Alert and Warning Systems (ISAWS), social media, reverse 911, and local radio and TV station messaging. Sending emergency messages over multiple systems is more effective than sending them over a single system. Careful consideration should be taken to ensure that non-emergency information is **not** sent via IPAWS Wireless Emergency Alert (WEA), EAS, or NWEM.

2.3 State Alerting

2.3.1 Idaho Office of Emergency Management

The Idaho Office of Emergency Management is responsible for coordinating statewide communications interoperability and emergency communications issues. As part of this function, IOEM facilitates statewide public alerting and assists local and state collaborative operating groups (COGs), alerting authorities, and alert originators.

IOEM serves as the state-level alerting official and works with local COGs to establish IPAWS public alerting applications (PAA) and memorandum of agreements (MOAs) with FEMA IPAWS officials. IOEM is Idaho's primary statewide alerting authority. However, IOEM utilizes the functionality and services of State Communications (STATECOMM) to generate and send alerts affecting statewide and regional jurisdictions.

IOEM works with partner agencies across the state to administer the overall public alerting program for the state of Idaho. IOEM specifically supports administrative oversight, publishing pertinent guidance, conducting education and outreach on public alerting, and working with the SECC to jointly administer the Idaho EAS plan.

The Idaho State Alert and Warnings System (ISAWS) is administered by IOEM to facilitate both emergency and non-emergency critical information thru a subscription-based service. Information on ISAWS can be obtained at www.isaws.org or by contacting IOEM directly. This program is separate from IPAWS and should not be confused with normal functions of IPAWs (EAS, WEA, etc.).

2.3.2 Idaho State Police

The Idaho State Police (ISP) are responsible for Amber Alerts, Blue Alerts, and Endangered Missing Persons Alerts. For activation information regarding criteria and plan, see Appendix C.

Additionally, ISP has the capability to send WEA for 911 Outage, Civil Danger, Civil Emergency, Evacuations, Local Area Emergency, and Shelter-in-Place scenarios, including active shooter incidents.

2.3.3 Idaho Department of Health and Welfare

State Communications (StateComm), is established by the Idaho Department of Health and Welfare, and serves as the primary communication entity for IOEM through a memorandum of agreement. StateComm is also authorized to provide alerts for local agencies. However, local agencies should consider the fact that StateComm may be unable to process alert requests in a timely manner if their workload is at a high level. Therefore, it is highly advisable that each local jurisdiction attempt to designate and train their own alerting authorities and originators. This empowers jurisdictions at the local level.

StateComm dispatch services encompass a wide range of responsibilities, including, but not limited to:

- Emergency Medical Services (EMS) dispatch and mutual aid coordination
- Idaho Department of Transportation (DOT) dispatch
- ITS (Intelligent Transportation Systems) for Idaho (e.g., DMS, CCTV, 511)
- Idaho Department of Fish and Game flight following
- Hazmat, logging, and dam incident response coordination
- Public Health Emergencies
- IPAWS: EAS, WEA, or NWEM activation
- Local assistance for WEA and EAS for evacuation (EVI) warnings for fire alerts
- Prehospital tissue referral notification
- Critical Incident Stress Management Team dispatch
- Search and Rescue dispatch

2.3.4 Collaborative Operating Groups (COGs)

The state IPAWS administrator approves COGs for certification through IPAWS. Additionally, the state IPAWS administrator collaborates with agencies on testing procedures and events for WEA broadcast messaging. The State Emergency Communications Committee (SECC) is a state level council designed to oversee Idaho's EAS plan and implementation. Collaborating together, the SECC and IOEM coordinate the testing of IPAWS for the EAS system, as well as resolve any issues that arise during these tests.

Each COG/agency approved by the state IPAWS administrator is an alerting authority authorized to use the FEMA IPAWS platform for emergency notifications.

Each established IPAWS COG maintains a list of all individuals who have successfully completed FEMA's IPAWS IS-247.b (as amended) course and other required courses as directed by federal guidance. Additionally, the list contains copies of completed course certificates, individual names/contact information, and copies of memorandum/resolutions officially designating these individuals as alert originators.

Per IPAWS rules, only one alerting authority will be authorized per county government, city government, and per each recognized tribal nation. Consideration will be given to include military installations on a case-by-case basis. This consideration will be given in coordination with local Emergency Management (EM) personnel and the state IPAWS administrator.

COG-level permissions can be found in Appendix B and describe the geographic boundaries for alerting, the types of alerts that can be issued, the alert approval process, and the dissemination systems that can be used to distribute such alerts. COG-level permissions help to define the area of responsibility and the capabilities the alerting authority has. The illustration below depicts the dissemination of alerting information.

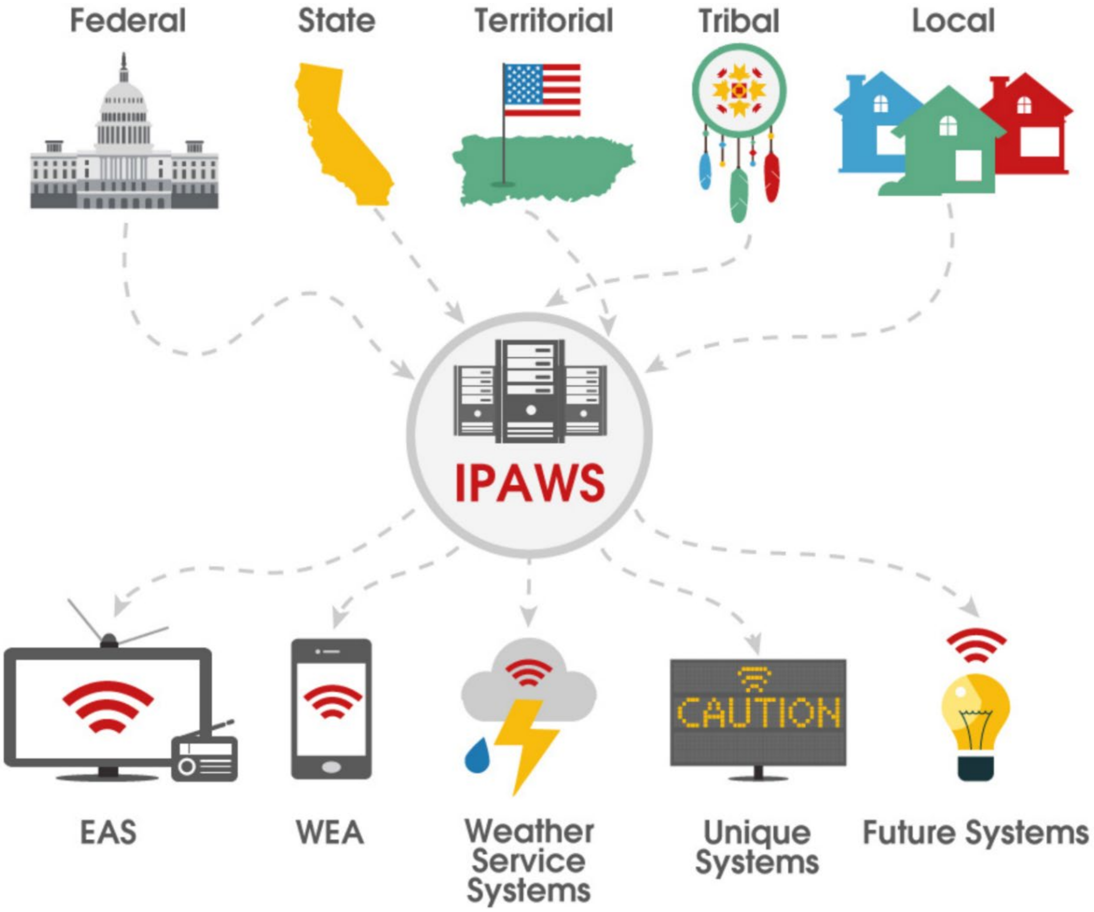


Figure 1: IPAWS Alerting Dissemination[1]

2.4 Federal Alerting

Federal alerting authorities, including the NWS, play a vital role in issuing public warnings about severe weather threats and other hazards. They use multiple systems to disseminate these warnings, such as NOAA Weather Radio All Hazards (NWR) and the EAS. The success of these public alerting and warning systems relies on the coordination between federal, state, and local agencies.

2.4.1 National Weather Service

[1] California Governor's Office of Emergency Services, IPAWS Figure, California Wireless Emergency Alerts - Alerting Authorities, 2014

The NWS is responsible for originating public warnings regarding weather hazards. The NWS operates several public alert and warning dissemination systems, including the National Weather Radio (NWR), a network of over 1,000 Very High Frequency (VHF) radio transmitters, NOAA Weather Wire Service (NWWS), and the Emergency Managers Weather Information Network (EMWIN). NWR is an all-hazards radio network, making it a single source for comprehensive weather and emergency information. In conjunction with federal, state, and local emergency managers and other public officials, NWR also broadcasts/conveys warning and post- event information for many types of non-weather hazards including natural incidents like earthquakes or avalanches, environmental incidents like chemical releases or oil spills, and public safety incidents like civil emergency messages or 911 telephone outages. Federal, state, and local officials may request directly to the NWS to broadcast other types of hazards.

The NWS requests activation of the EAS for imminent and dangerous weather conditions, uses NWR as its primary means to activate EAS, and can assist with relaying state and local authorities' non-weather EAS messages and activations via NWR. The NWR can communicate important NWEM, such as 911 outages, shelter-in-place, and civil emergency messages. While the NWS is responsible for weather-related alerting, local government is not precluded from sending NWEM notifications and alerts in support of weather events. Authorized state and local government originators may use IPAWS to issue NWEM via NWR.

It is voluntary for EAS participants, such as radio and television stations, to further relay NWS-generated messages, except in cases of national-level activation of the EAS. NWS EAS codes can be found at: https://www.weather.gov/nwr/eventcodes.

2.4.2 Federal Communications Commission

The FCC, in conjunction with FEMA and NOAA NWS, implements the EAS at the federal level. The FCC's role includes establishing technical standards for EAS participants, procedures for EAS participants to follow in the event the system is activated, and testing protocols for EAS participants.

2.4.3 Federal Emergency Management Agency

FEMA is responsible for all national-level activation, tests, and exercises for the EAS. The EAS is a national public warning system that utilizes radio and television broadcasters, cable systems, satellite radio and television providers, and wireline video providers. FEMA maintains and operates IPAWS. IPAWS is FEMA's national system for local alerting that provides authenticated emergency and life-saving information to the public through mobile phones using WEA and radio and television via the EAS and the NWR. IPAWS was established under Executive Order 13407. IPAWS provides the capability to notify the public of impending natural and human-made disasters, emergency, and public safety information. FEMA provides 24/7 technical support for IPAWS users and is responsible for issuing credentials for use of the system.

3. Technologies

3.1 Integrated Public Alert and Warning System (IPAWS)

FEMA IPAWS is an internet based common alerting protocol which enables and standardizes alerting for federal, state, local, and tribal entities. It is primarily comprised of the EAS, WEA, and the National Weather Service alerting platforms for weather and non-weather alerts. In the case of EAS and WEA, a third-party software service is required to actually format and publish alerts and must be compatible with IPAWS alerting protocol. Appendix D lists the software applications that are compatible and have been tested with IPAWS.

The process for signing up and becoming a recognized COG and alert originator is described in Appendix B. During the course of this process, the state IPAWS administrator will review the Public Alerting Application (PAA) and determine which event codes a given alert originator will be authorized to utilize. Event codes, such as EQW (Earthquake Warning), are generally assigned based on known historical or existing probable threats. Additionally, the state IPAWS administrator will verify with FEMA and the county the specific Federal Information Processing Standard (FIPS) code to use. FIPS codes are unique numbers used to identify specific states, counties, and geographic areas.

It should be noted that although IPAWS is a preferred platform for alerting, it is not the only means of alerting the public. There are many other systems and procedures that can be implemented in concert with IPAWS or utilized separately. More detailed information on IPAWS can be found here: www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system.

3.2 Emergency Alert System (EAS)

Counties can effectively utilize the EAS by coordinating with their State Primaries (SP) to distribute emergency alerts through broadcasters and cable operators. Local jurisdictions with authorized IPAWS COGS to issue EAS alerts independently within their jurisdiction may also do so. It is crucial for counties to establish procedures with their agencies responsible for originating alerts through the State Primary or locally via IPAWS. Collaboration and adherence to established protocols will ensure a streamlined and effective emergency alert process. Under certain unusual conditions (such as SP and IPAWS unavailability) designated local broadcasters (Local Primaries or LPs) may be used for issuing EAS alerts. However, LPs can only activate EAS (not WEA, etc.) and only for counties within their Local Area EAS Plans. Further information and guidance regarding EAS issuance can be found in the Idaho EAS Plan.

3.3 Emergency Mass Notification Systems (MNS)

Localities can effectively communicate with residents through telephone notification systems by having the ability to target specific areas, draw from opt-in data and publicly available directories, and disseminate detailed warning information. However, there may be limitations in terms of the time required to execute all calls due to infrastructure constraints, message length, or technological issues. It is crucial for alerting authorities to collaborate with local telecommunications providers to understand these limitations and tailor their message delivery accordingly to ensure successful communication with recipients in times of emergency. By working together and being mindful of these factors, authorities can enhance the efficiency and effectiveness of their alerting systems.

To maximize the reach of telephone notification systems, alerting authorities should take advantage of features such as automatic voicemail options for unanswered calls and the option to include voice recordings on an Audio Bulletin Board. By utilizing both functionalities, authorities can increase the likelihood of recipients receiving important messages and ensure effective communication during emergency situations. Opting for a multi-faceted approach enhances the system's ability to reach a wider audience and can improve overall emergency preparedness and response efforts.

Finally, these systems can use a variety of other communication mediums including Short Message Service (SMS) and Short Message Peer-to-Peer (SMPP) text messages, emails, fax, telecommunications devices for the deaf (TDD)/teletypewriter (TTY), and others. To optimize communication efforts during emergencies, it is recommended to utilize all available contact methods when sending a message and configure the system to request confirmation of message receipt. This approach ensures that the system exhausts all possible communication channels until it receives positive acknowledgment from the recipient, thereby enhancing the effectiveness of emergency notifications and response strategies.

4. Public Alerts and Warnings Best Practices

All disasters and emergencies are locally oriented. While first responders are preparing to or responding to an incident, it is an inherent responsibility of local officials to keep the public informed of what actions they need to take to protect themselves. Communicating these instructions to the public is the primary purpose of IPAWS. Because local officials have a better understanding of the situation, the immediate actions that are being taken, and potential adverse impacts of the incident, they play a crucial role in conveying vital information.

There is no one-size-fits-all formula for determining messaging strategies. However, there are evidence-based principles and best practices available to assist decision-makers in making informed choices:

- Utilization of alerting mechanisms within the IPAWS should be a primary route to issue emergency alerts and warnings to ensure the greatest number of recipients within the impacted area are being alerted.
- The responsibility for issuing alerts and warnings during an emergency rests with designated public officials, known as the Alerting Authority, at the county, state, and tribal level. It is their decision to determine who authorizes the issuance of alerts and/or warnings.
- Unless otherwise notified, Sheriff Offices (SOs), PSAPs, and county emergency management agencies are generally considered to be the most recognized primary alerting authority for their jurisdictions.
- Incomplete or imperfect information is not a valid reason to delay or avoid issuing a warning. Time is of the essence, as recipients of warnings will need time to consider, plan, and act after they receive a warning message. This is particularly true among individuals with disabilities and people with access and functional needs, as they may require additional time to evacuate or may be at increased risk of harm without notification.
- Messages should come from an authoritative source and clearly identify the originating agency.
- Whenever possible, messages should help the target audience recognize that the Alerting Originator is knowledgeable about the threat.

- Warning messages can, and should be, updated and refined as additional information becomes available. Additionally, when the threat or warning messages are no longer applicable, a message stating that it no longer applies should be sent.
- Warning messages sent in error should be updated, clarified, or retracted quickly from the message being confirmed as being erroneous.

4.1 Delivery of Messages to Populations with Additional Communications Needs and Non-English-Speaking Individuals

To the extent possible, 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 make all information accessible to their constituents, including emergency alerts and warnings. 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, non-English-speaking, persons with intellectual or developmental disabilities, or any others who receive and/or process information in alternate ways. Emergency alerts and warnings should account for the wide array of communication needs found in the public. For additional information, see the ADA’s Emergency Planning webpage.

Alerting Authorities should seek resources such as the Department of Health and Human Services or other similar agencies to explore opportunities to deliver messages to everyone who needs them, including through non-conventional methods.

5. Alert Decision Making

5.1 Guidance for Issuing Social Media Alerts

Social media is now a critical component for disseminating emergency messaging, instructions, and recovery information to both the media and the public. Due to its unique nature, it functions instantaneously and creates the appearance of highly official two-way dialogue between the agency and very large groups of people, including news media and stakeholders. Messaging for social media must be very carefully managed. Social media has the capability to deliver text, audio, video, images, infographics, maps, and other data and requires a skill set of regular use. These platforms have inherent expectations for two-way engagement and therefore demand more staff time and resources.

Social media is more successful when the community is engaged, and official accounts have established themselves as credible sources of information. Methods of engagement may include:

- Awareness campaigns
- Personalized responses to questions and comments
- Image sharing and messaging
- Video sharing
- Blogging and Vlogging

- Live events

Considerations for incorporating social media into alerts and warnings before, during, and after emergencies include:

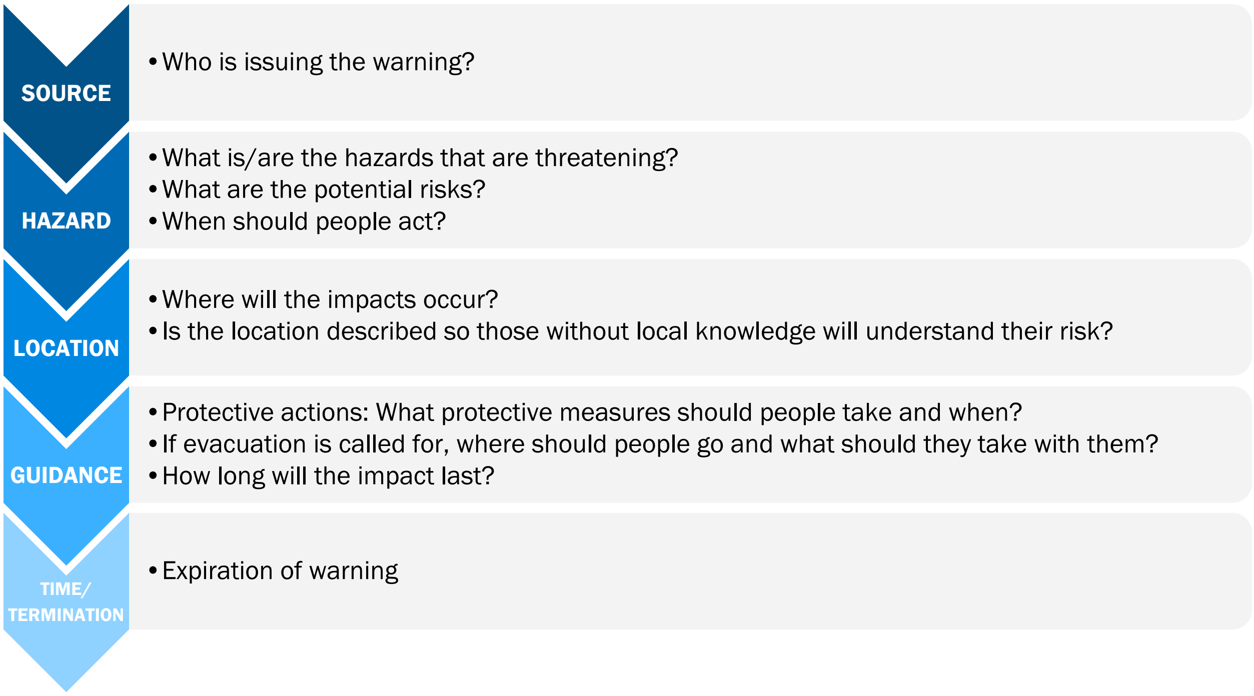
- Social media outreach is highly dependent on working cellular and data networks that may be impaired or down during and following an emergency.
- Consider the variety of languages and the complexity of language to use in postings.
- Social media is highly effective at reaching the news media, which may assist in more broadly sharing messaging.
- Briefings and updates via live and recorded video are recommended when internet access and bandwidth allow.
- 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.
- 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.
- Ensure that there is a process in place to address reports of emergencies (imminent threats to health and welfare, reports of citizens trapped or injured, and third-party reports of people in danger or a prolonged period of non-contact) to all the previously mentioned social media platforms.
- Updating the original post with new information is recommended to maintain current information when shared by others, eliminating the need for the public to share a new post with the update.
- Amplify alerts and warnings by commenting and sharing posts by other agencies.

5.2 Guidance for Issuing Wireless Emergency Alerts (WEA) Messages

Wireless Emergency Alerts (WEAs) are short emergency messages from authorized federal, state, local, tribal, and territorial public alerting authorities that can be broadcast from cell towers to any WEA-enabled mobile device in a locally targeted area. When circumstances arise and there is a need for a public warning, the decision to send a message is ultimately a matter of local judgment. To assist in the decision-making process, the following criteria may be applied:

- Does the hazardous situation require the public to take immediate action?
- Does the hazardous situation pose a serious threat to life or property?
- Is there a high degree of probability the hazardous situation will occur or escalate?

If the answer to all the questions above is “yes” and the decision is made to issue an alert, then information on the source, hazard, location, guidance, and time/termination should be included in the message. Please note that based on IPAWS version status, the Alerting Authority may be limited to 90 characters. All alerts should include a 90- and 360-character message. The questions in Figure 2, below, should also be taken into consideration when disseminating a WEA message.



SOURCE

- Who is issuing the warning?

HAZARD

- What is/are the hazards that are threatening?
- What are the potential risks?
- When should people act?

LOCATION

- Where will the impacts occur?
- Is the location described so those without local knowledge will understand their risk?

GUIDANCE

- Protective actions: What protective measures should people take and when?
- If evacuation is called for, where should people go and what should they take with them?
- How long will the impact last?

TIME/ TERMINATION

- Expiration of warning

Figure 2: WEA Message Guideline

IOEM follows best practices and ensures all messages are reviewed by at least one person other than the individual that created it prior to sending the message. This process includes reviewing grammar and message settings. Local jurisdictions are encouraged to follow the same procedure. To access tools and templates provided by FEMA to assist in generating messages, visit: https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public-safety-officials/toolkit/templates

Additionally, see below for Alerting Authority example messages.

Example Messages:

"(Blank) County Emergency Management. Chlorine gas release at 700 Sandridge Rd (city/town). Toxic Cloud moving toward Madison Park. Breathing this gas will result in immediate death. Close doors and windows and turn off Air Conditioning. Drivers remain in vehicles. This must be completed in the next 10 minutes. This message will expire at XXXX am."

"From: (Blank) County Emergency Management. Armed suspect at 700 Sandridge Rd (city/town). Stay indoors and secure all windows and doors, report all suspicious activity to 911. Tune in to local media for more information."

"From: (Blank) County Emergency Management. I-29 near mile marker 77 is currently closed due to flooding. Be patient. Do not call 911 unless you have an emergency, Keep the emergency lane open! Tune into local media for more information."

5.3 Emergency Notifications Usage

Emergency notification refers to a life-threatening or serious property-threatening event or condition. They are often issued throughout the response based on need.

IOEM and/or local agencies may issue emergency notifications for life-threatening or serious property-threatening events or conditions based on the observations of its staff, or at the request of other public safety agencies.

5.4 Non-Emergency Information Usage

Not all messages are of an urgent and life-threatening nature, so alerting authorities should consider the use of other means of passing more routine or non-critical information along to the public. Examples may include utilizing social media, press releases, outdoor signage (electronic or physical), website blogs, etc. Some local jurisdictions may have laws, local ordinances, regulations, or specific policy pertaining to this type of messaging. It is also implied that when time permits, most messaging may need approval by the designated chain of supervision. As the urgency or critical nature of the messaging increases, so will the likelihood of a more intense or formal approval method.

As with any public alerting, consider the key elements of information to include within the message. Indicate the nature of the message (i.e. road closures, restrictions, updates), what you want the public to do, when the message applies, and where to get more information.

5.4.1 Prohibited Non-Emergency Notifications

The following non-Emergency Notifications are prohibited:

- Any message of a commercial or “for profit” nature
- Any message of a political nature, even the hint of political favoritism is discouraged
- Any non-official business not related to the emergency
- The use of any individual's specific name not related to a public safety condition or event

5.5 Alerting Coordination

When considering issuing an alert and/or warning to the public, jurisdictional coordination, communication, and collaboration should be a priority. As much as possible, warning coordinators should ensure that warnings are targeted to the area known to be at risk while also coordinating with any other affected jurisdictions as soon as possible. If the initial warning originator lacks the ability to deliver warnings to the at-risk area, coordination with other jurisdictions should be given priority. Alerting for another jurisdiction is accomplished by having an agreement in place with the other jurisdiction on the following:

- Establishing how alerting will be activated
- Establishing agreed-upon alerting criteria
- Establishing procedures for alerting
- Updating the Public Alerting Authority document with FEMA IPAWS to include the other jurisdiction and notify vendors of the change so they can update the software and allow alerts for the additional geographical area

5.5.1 Cross-jurisdictional Alerting

To ensure efficient and effective cross-jurisdictional alerting, it is strongly recommended that agencies establish formal agreements that outline the parameters for such coordination. These agreements should address key aspects such as circumstances for cross-jurisdictional alerting, roles of partner agencies, agreed-upon alerting criteria, procedures for alerting, and mechanisms to overcome barriers such as permissions within the system, shared IPAWS Specific Area Message Encoding (SAME) codes, technical barriers, training requirements, and considerations regarding privacy, security, and legal compliance. By having a structured framework in place, partner agencies can collaboratively navigate through potential challenges and ensure seamless communication during emergency situations across different jurisdictions.

5.6 Erroneous or False Alert Procedures

Structured training and practice are vital to reduce the risk of false alerts. False alerts are damaging to the credibility of both the source agency and the method used. False alerts and/or erroneously issued warnings can cause the public to question the accuracy of future messages.

If an erroneous, false, or misleading message is sent, the public in the alerted area should be notified immediately, and any protective measures recommended should be disregarded. Alerting authorities should have procedures in place for such an event. In the case of an erroneous alert or warning, it is recommended that the issuing agency head be immediately notified. Likewise, the Idaho State EMS Communications Center (StateComm) should be notified for situational awareness.

Broadcasters and cable companies are required to notify the FCC of a false EAS alert within 24 hours of becoming aware of the false alert. State or local government originators are encouraged to do so as well. The notification can be sent to the FCC Public Safety and Homeland Security Bureau (PSHSB) 24/7 Operations Center:

- FCCOps@fcc.gov
- (202) 418-1122

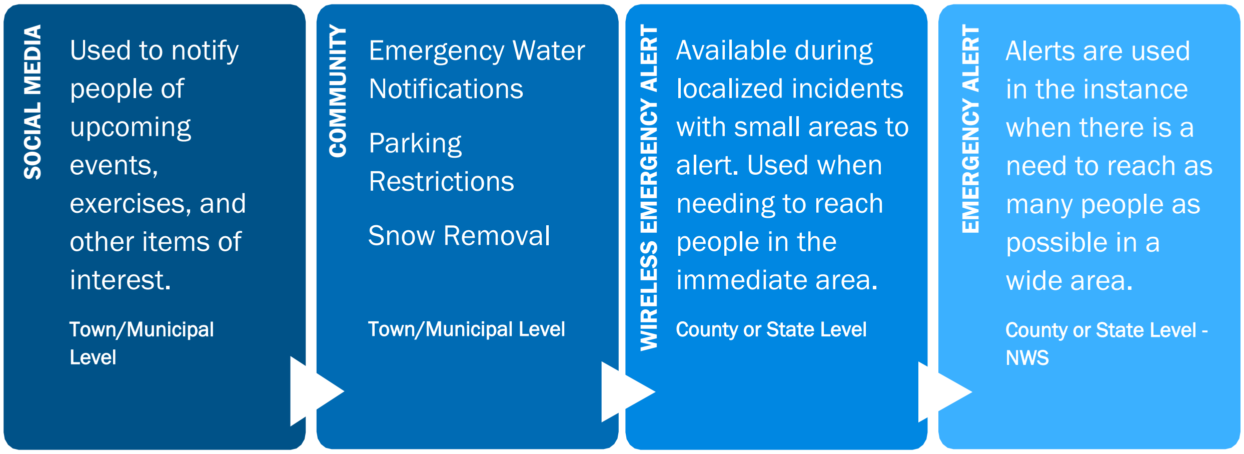
5.7 Use of Multiple Alerting Technologies and Strategy

Many agencies have multiple notification/alerting systems that can be used to deliver both emergency and non-emergency information to their communities. Although tool reach overlaps may happen, each of these systems can also target a unique demographic in a region that other methods may not be able to reach. It is therefore the Alert Authorities' responsibility to choose the tools necessary to reach the specific segments of the population, depending on the scope and scale of the event precipitating the notification.

In general, the larger and more dangerous the event, the more tools will be employed. Care should be taken to not inundate the population with too many notifications, but due regard must be given to the necessity of alerting ALL of the people in an area affected by an emergency. It is advisable to address this division of responsibilities before an emergency happens by having authorities create messaging strategies, establish thresholds, decision points, approval processes, and procedures in advance of any incident. These strategies should be well informed by emergency communications center personnel, emergency managers, public safety leaders, members of the community, and telecommunications providers in an area.

By setting an inclusive strategy well in advance, publicizing it, training for it, exercising for it, and employing it during an incident, jurisdictions are much more likely to strike a balance between under- and over-alerting a message.

In all cases, careful consideration should be taken to ensure that non-emergency information is NOT sent via IPAWS, including WEA and EAS. Jurisdictions may find the chart below helpful when deciding what methods to use to disseminate information.



SOCIAL MEDIA

Used to notify people of upcoming events, exercises, and other items of interest.

Town/Municipal Level

COMMUNITY

Emergency Water Notifications

Parking Restrictions

Snow Removal

Town/Municipal Level

WIRELESS EMERGENCY ALERT

Available during localized incidents with small areas to alert. Used when needing to reach people in the immediate area.

County or State Level

EMERGENCY ALERT

Alerts are used in the instance when there is a need to reach as many people as possible in a wide area.

County or State Level - NWS

Figure 3: Methods of Dissemination

5.7.1 Dissemination Channels

The effectiveness of emergency communication channels depends on various factors, including speed, coverage, concentration, and how comprehensive messages are. Tables 2A, 2B, and 2C, below, provide a comparison of different dissemination channels, categorized by speed, to help identify the most suitable channels for emergency communications.

Table 2A: Speed - Very Slow/Slow/Moderately Fast

Dissemination Channels	Speed	Coverage	Concentration	Message Comprehensiveness
Newspaper	Very Slow	Widespread	Dispersed	Very High
Route Alerting / Door to Door	Slow	Limited	Concentrated	High
Radio	Moderately Fast	Widespread	Dispersed	High to Low
Television Broadcast	Moderately Fast	Widespread	Dispersed	Very High to Medium
Television Message Scrolls	Moderately Fast	Widespread	Dispersed	Low

Table 2B: Speed - Fast

Dissemination Channels	Speed	Coverage	Concentration	Message Comprehensiveness
Loudspeakers and Public	Fast	Limited	Concentrated	Medium

Dissemination Channels	Speed	Coverage	Concentration	Message Comprehensiveness
Address (PA) Systems				
Dedicated Tone Alert Radios	Fast	Limited	Concentrated	High
Tone alert and NOAA Weather Radio	Fast	Widespread	Dispersed	High
Text Telephone (TDD/TTY)	Fast	Widespread	Dispersed	Low
Reverse Telephone Distribution Systems	Fast	Widespread	Dispersed	High
Audio Sirens and Alarms	Fast	Limited	Concentrated	Very Low
Broadcast Sirens	Fast	Limited	Concentrated	Medium
Message Boards	Fast	Limited	Concentrated	Low
Visual Alerting	Fast	Limited	Concentrated	Low
Internet Protocol (IP) Based technology	Fast	Widespread	Dispersed	Very High to Medium
Social Media	Fast	Widespread	Dispersed	Low

Table 2C: Speed - Very Fast

Dissemination Channels	Speed	Coverage	Concentration	Message Comprehensiveness
WEA	Very Fast	Widespread	Dispersed	Very Low
Wireless communications (SMS)	Very Fast	Widespread	Dispersed	Very Low

6. System Operations

6.1 System Management

If an agency has an IPAWS MOA with FEMA and is an approved COG, it is assigned a COG Identification (ID) and authority to alert one or more Federal Information Processing Standard (FIPS) county codes. There are two keys for IPAWS, the first being a training key and the other the live key.

- The training key will allow a user to sign in to IPAWS through IPAWS-capable software but will not send an IPAWS alert.
- The live key is used when conducting tests of IPAWS or for an actual IPAWS alert. The live key should never be used for training.

Upon the separation of an employee who had access to the training key or live key, or when the password is suspected or known to have been compromised, both passwords must be changed immediately by the local system administrator or by contacting the system vendor if the system administrator does not have those capabilities.

It is imperative that all software used to access IPAWS, EAS, WEA, or other messaging systems be maintained and kept updated when software updates are released to ensure that access, functionality, and security of alerting access is maintained.

6.2 System Security

Every system user is responsible for access security as it relates to their use of IPAWS/WEA messages and shall abide by these Rules of Behavior:

- All users must have a discrete user account ID for login which cannot be the user's social security number. To protect against unauthorized access, passwords and user ID are linked and used to identify and authenticate authorized users.
- Accounts and passwords shall not be transferred or shared. The sharing of both a user ID and associated password with anyone (including administrators) is prohibited.
- Accounts and passwords shall be protected from disclosure, and writing passwords down or electronically storing them on a medium that is accessible by others is prohibited.
- Passwords must not contain names, repetitive patterns, dictionary words, product names, personal identifying information (e.g., birthdates, social security numbers, phone number), and must not be the same as the user ID.
- Passwords must be greater than eight numbers, letters, or characters.
- Passwords must be promptly changed whenever the compromise of a password is known or suspected.

6.2.1 Users Accessing IPAWS:

- Physically protect computing devices such as laptops, computer gaming consoles, smartphones etc.; protect sensitive data sent to or received from IPAWS; and do not program computing devices with automatic sign-on sequences, passwords, or access credentials when using IPAWS.
- Users will not provide or knowingly allow other individuals to use their account credentials to access IPAWS.

- To prevent and deter others from gaining unauthorized access to sensitive resources, users will log off or lock their computer workstation, or will use a password-protected screensaver whenever the user steps away from a workstation area. Preventative measures shall be taken even if the user is only leaving for a short time, and users will log off when leaving for the day.
- Inform the local system administrator when access to IPAWS is no longer required.
- Promptly report security incidents to the Local System Administrator and the state IPAWS coordinator.
- All employees shall receive cybersecurity awareness training and should follow cybersecurity best practices in protecting both IPAWS physical access equipment and network access.
- Only trained and certified users shall be allowed access to the IPAWS software.

6.3 Training and Testing

To ensure effective and efficient use of alerts and warnings capabilities, agencies must regularly train and exercise their alerts and warnings policies, procedures, and systems. Any member of an alert authority whose duties include disseminating public AWN must complete all required FEMA Independent Studies course(s) at the time of application or renewal. They are responsible for ensuring and documenting that their designated users are properly trained and that all certifications are current. To facilitate the annual training requirement, IOEM coordinates training with local alert originators.

System administrators are encouraged to develop custom training curriculums based on custom roles created. Additional training can be found through current vendor resources.

6.3.1 Local IPAWS Tests

In accordance with FEMA guidance, alert originators are required to perform a monthly test alert to the IPAWS Message Lab testing platform. They can perform this test by using a COG test ID issued by FEMA. This allows alert authorities to send an actual WEA message, with real alerting codes, in a safe testing environment.

Each alert authority must adopt a monthly testing plan to ensure operational readiness. They should conduct regular training and exercises, including tests of all components of the AWN program to ensure the ability to send emergency notification information across the entire program. Any impediments should be identified and a resolution at the lowest jurisdictional level possible should be developed.

Please note:

- Live messages sent to the production environment WILL NOT be considered for Monthly Proficiency Demonstration scoring.
- If a COG misses a single Monthly Proficiency Demo, they will receive a reminder from FEMA.
- If a COG misses two consecutive Monthly Proficiency Demos, then both they and their state IPAWS Reviewing Authority will be notified.
- If a COG misses three consecutive Monthly Proficiency Demos, they will LOSE ACCESS to the IPAWS Live Production Environment and WILL NOT be able to use IPAWS for public alerting until such a time as they complete a successful Monthly Proficiency Demo.
- If a COG does not reinitiate proficiency testing, they will be removed from the IPAWS program and be ineligible for MOA renewal until deficiencies are corrected and personnel retrained.

Jurisdictions should assess every component of their alerts and warnings program and identify the appropriate testing cycles for each piece. Systems that are used frequently (at least monthly) may not require system testing frequencies as aggressive as those that are used less frequently.

It is important to understand testing limitations. For example, it is not allowable to test on unlisted or 911 database phone numbers.

7. Alert Guidelines

7.1 Weather and Non-Weather Emergency Message Guidelines

The Integrated Public Alert and Warning System aids federal, state, local, tribal, and territorial public safety agencies in disseminating WEAs, EAS alerts, and weather and non-weather-related emergency messages concurrently through various channels such as NOAA weather radios, sirens, and digital billboards.

The IPAWS Administrator establishes protocols for the use of alert codes by authorized agencies, specifying the approved codes granted through the application process. These agencies are permitted to utilize the standardized alert codes provided by IPAWS, as well as designated testing codes. For further information on IPAWS and the application process, please refer to Appendix B.

Additionally, Idaho employs non-weather emergency messages for public communication. The guidelines for the appropriate use of Weather and Non-Weather alerts are detailed in Table 3, below.

Table 3: Weather and Non-Weather Event Codes

Alert	Criteria
911 Telephone Outage Emergency (TOE)	An emergency message that defines a local or state 911 telephone network outage by geographic area or telephone exchange.
Avalanche Watch (AVA)	A warning of imminent or occurring avalanche activity.
Blizzard Warning (BZW) ***NOAA**	**A warning issued when falling and/or blowing snow reduces visibilities to less than 1/4-mile sustained winds, or frequent gusts to 35 mph or higher are present, or there are conditions persisting for three hours or longer.**
Blue Alert (BLU)	A message issued to warn the public when there is actionable information related to a law enforcement officer that is missing, seriously injured, or killed in the line of duty, or when there is an imminent, credible threat to an officer. A Blue Alert can quickly warn the public if a violent suspect may be in the community and provide instructions on what to do if the suspect is spotted and how to stay safe. See Appendix C for information on requesting alerting authority. ** **Idaho State Police, StateComm, and the NCMEC are the only alerting authorities for these messages. COGS should coordinate with above authorities for issuance.

Alert	Criteria
Child Abduction Emergency (CAE)	Based on established criteria, an emergency message about a missing child believed to be abducted. A local or state law enforcement agency investigating the abduction will describe the missing child, provide a description of the suspect and/or vehicle, and ask the public to notify the requesting agency if they have any information on the whereabouts of the child or suspect.** **Idaho State Police, StateComm, and the NCMEC are the only alerting authorities for these messages. COGs should coordinate with above authorities for issuance.
Civil Danger Warning (CDW)	A warning of an event that presents a danger to a significant civilian population. The CDW, which usually warns of a specific hazard and gives specific protective action, has a higher priority than the Local Area Emergency (LAE).
Civil Emergency Message (CEM)	An emergency message regarding an in-progress or imminent significant threat(s) to public safety and/or property. The CEM is a higher priority message than the Local Area Emergency (LAE), but the hazard is less specific than the Civil Danger Warning (CDW).
Dust Storm Warning (DSW) ***NOAA**	**A warning when blowing dust is expected to frequently reduce visibility.**
Earthquake Warning (EQW)	A warning of current or imminent earthquake activity. Authorized officials may recommend or order protective actions according to state law or local ordinance.
Evacuation Immediate (EVI)	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 approaching tropical cyclone. In the event a flammable or explosive gas is released, authorized officials may recommend evacuation of designated areas where casualties or property damage from a vapor cloud explosion or fire may occur.
Fire Warning (FRW)	A warning that indicates a spreading wildfire or structure fire threatens a populated area. Evacuation of areas in the fire's path may be recommended by authorized officials according to state law or local ordinance.
Flash Flood Warning (FFW) ***NOAA**	**A warning issued when flash flooding is imminent or occurring.**
Hazardous Materials Warning (HMW)	A warning indicating the release of a nonradioactive hazardous material (such as a flammable gas, toxic chemical, or biological agent) that requires the public to evacuate from the affected area (for an explosion, fire, or oil spill hazard) or shelter in place (for a toxic fume hazard).

Alert	Criteria
High Wind Warning (HWW) ***NOAA**	**A warning issued when the following conditions are expected: when there are sustained winds of 40 mph or higher for one hour or more, or there are wind gusts of 58 mph or higher for any duration.**
Law Enforcement Warning (LEW)	A warning of a bomb explosion, riot, or other criminal event (e.g., a jailbreak). An authorized law enforcement agency may blockade roads, waterways, or facilities, evacuate or deny access to affected areas, or arrest violators or suspicious persons.
Local Area Emergency (LAE)	An emergency message that defines an event that, by itself, does not pose a significant threat to public safety and/or property. However, the event could escalate, contribute to other more serious events, or disrupt critical public safety services. Instructions, other than public protective actions, may be provided by authorized officials. Examples include a disruption in water, electric, or natural gas service, a significant interruption in a transportation artery or a potential terrorist threat where the public is asked to remain alert.
Missing and Endangered Person(s) (MEP)	An alert issued for individuals who are at risk of harm due to their circumstances. These individuals may be incapable of returning to their residence without assistance due to mental or physical incapacities, including mental illness, intellectual disability, dementia, or physical limitations. Alerts may also be issued for individuals who have gone missing under suspicious, involuntary, or unexplained circumstances, or those whose disappearance may be related to the commission of a crime. Additionally, alerts may be issued for individuals who need medical attention or prescription medication, have previously been the victim of violence or threats, or are in inherently dangerous situations. See Appendix C for more information on requesting alerting authority. ** **Idaho State Police, StateComm, and the NCMEC are the only alerting authorities for these messages. COGs should coordinate with above authorities for issuance.
Nuclear Power Plant Warning (NUW)	A warning of an event at a nuclear power plant. Classified as a Site Area Emergency or General Emergency by the Nuclear Regulatory Commission (NRC). A Site Area Emergency is confined to the plant site, and no offsite impact is expected. Typically, a General Emergency is confined to a less than 10-mile radius around the plant.
Practice/Demo Warning (DMO**) EAS, NWEM Only	A demonstration or test message used for purposes established in state, including local, tribal, or territorial, EAS plans. Purposes may include testing of a siren system or audio quality checks.
Radiological Hazard Warning (RHW)	A warning of the loss, discovery, or release of a radiological material.

Alert	Criteria
Required Monthly Test (RMT) EAS Only	A test message that is typically prescheduled and coordinated state- or region-wide on a monthly basis. RMTs generally originate from a pre-designated local or state primary station, or a state emergency management agency.
Required Weekly Test (RWT) EAS Only	The "required" weekly test is not a requirement for Public Safety organizations as it is for our broadcast and cable partners. Required weekly tests are used to verify EAS activation in the same manner silent testing (air) tests are performed on outdoor warning sirens. Local COGs who plan on using EAS are encouraged to periodically test with required weekly test.
Severe Thunderstorm Warning (SVR) ***NOAA**	**A warning issued when severe thunderstorms are occurring or imminent in the warning area.**
Shelter in Place Warning (SPW)	A warning of an event where the public is recommended to shelter in place (go inside, close doors and windows, turn off air conditioning or heating systems, and turn on the radio or TV for more information).
Tornado Warning (TOR) ***NOAA**	**A warning issued when a tornado is imminent.**
Volcano Warning (VOW)	A warning of current or imminent volcanic activity. Authorized officials may recommend or order protective actions according to state law or local ordinance.
Winter Storm Warning (WSW) ***NOAA**	**A warning issued when a significant combination of hazardous winter weather is occurring or imminent.** **Significant and hazardous winter weather is defined as a combination of:** **1) Five inches or more of snow/sleet within a 12-hour period *or* seven inches or more of snow/sleet within a 24-hour period,** **AND/OR** **2) Enough ice accumulation to cause damage to trees or powerlines,** **AND/OR** **3) A life threatening or damaging combination of snow and/or ice accumulation with wind.**
***Bold** = Weather Event	

Appendix A: Acronyms and Definitions

Acronym	Definition
ADA	Americans with Disabilities Act
AWN	Alerts, Warnings, and Notifications
BZW	Blizzard Warning
CAE	Child Abduction Emergency
CAP	Common Alerting Protocol
CDW	Civil Danger Warning
CEM	Civil Emergency Message
CISA	Cybersecurity and Infrastructure Security Agency
COG	Collaborative Operating Group
DHS	U.S. Department of Homeland Security
DIGB	District Interoperability Governance Board
DMO	Practice/Demo Warning
DOT	Department of Transportation
DSW	Dust Storm Warning
EAN	Emergency Action Notification
EAS	Emergency Alert System
EM	Emergency Management
EMS	Emergency Medical Services
EMWIN	Emergency Managers Weather Information Network
EQW	Earthquake Warning
EVI	Evacuation Immediate
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FFW	Flash Flood Warning
FIPS	Federal Information Processing Standards
FRW	Fire Warning
HMW	Hazardous Materials Warning
HWW	High Wind Warning
ID	Identification
IOEM	Idaho Office of Emergency Management
IPAWS	Integrated Public Alert and Warning System
IPSCC	Idaho Public Safety Communications Committee
ISAWS	Idaho State Alert and Warning System
IT	Information Technology
ITS	Intelligent Transportation System

Acronym	Definition
LAE	Local Area Emergency
LEW	Law Enforcement Warning
LP	Local Primaries
MOA	Memorandum of Agreement
NAWAS	National Warning System
NIC	National Information Center
NMN	Network Message Notification
NOAA	National Oceanic and Atmospheric Administration
NPT	National Periodic Test
NUW	Nuclear Power Plant Warning
NWEM	Non-Weather Emergency Message
NWR	NOAA Weather Radio
NWS	National Weather Service
PAA	Public Alerting Application
RHW	Radiological Hazard Warning
RMT	Required Monthly Test
RWT	Required Weekly Test
SECC	State Emergency Communications Committee
SMPP	Short Message Peer-to-Peer
SMS	Short Message Service
SO	Sheriff’s Office
SOP	Standard Operating Procedure
SP	State Primaries
SPW	Shelter in Place Warning
STATECOMM	State EMS Communications Center
SVR	Severe Thunderstorm Warning
SWIC	Statewide Interoperability Coordinator
TDD	Telecommunications Devices for the Deaf
TOE	911 Telephone Outage Emergency
TOR	Tornado Warning
TTY	Teletypewriter
VHF	Very High Frequency
VOW	Volcano Warning
WEA	Wireless Emergency Alert
WSW	Winter Storm Warning

Appendix B: IPAWS Application Process

The state IPAWS administrator at IOEM approves applications for IPAWS Alerting Authorities within the state. Agencies desiring to obtain alerting authority must contact the state IPAWS administrator prior to purchasing any software or equipment. The state IPAWS administrator ensures that adequate and proper alerting responsibilities are assigned. Copies of all documents referenced below are available from the state IPAWS administrator.

How to apply for IPAWS:

1. Contact the state IPAWS administrator for prior approval and guidance.
2. Select an IPAWS-compatible software. Access to IPAWS is free, but to send a message using IPAWS, an organization must procure its own IPAWS-compatible software. A list of private sector developers can be found at: www.fema.gov/sites/default/files/documents/fema_alert-origination-software-providers-ipaws_102022.pdf.
3. Apply for an MOA with FEMA at https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public-safety-officials/sign-up.
    a. To become a COG, an MOA governing system security must be executed between the sponsoring organization and FEMA. Each MOA is specifically tailored to the sponsoring organization and their interoperable software system.
4. The MOA will be sent as part of the FEMA application process. The FEMA COG coordinator will prepare and return the MOA for signature after it is submitted and assign a COG ID. After being signed by the applicant, the MOA will be routed for FEMA signatures. A copy of the executed MOA and the COG-specific digital certificate will be returned to the sponsoring organization. Both the COG ID and digital certificates (live and test) are necessary to configure the IPAWS-compatible software system.
5. Complete IPAWS web-based training:
    a. Complete IS-247.b at: https://training.fema.gov/is/courseoverview.aspx?code=is-247.c&lang=en
    b. Send the Certificate of Achievement to the contact below:

        The Idaho Office of Emergency Management
        Sid Brown, IOEM Emergency Communications Program Manager
        sbrown@imd.idaho.gov
6. Apply for public alerting permissions:
    a. Applicants will receive a public alerting application along with the unsigned MOA. The designated state official must sign this application.
    b. Complete the application, defining the types of alerts a COG intends to issue and the extent of its geographic warning area. The contact information for the designated state reviewer will be provided with the public alerting application.
    c. This form should be submitted for approval to:

        The Idaho Office of Emergency Management
        Sid Brown, IOEM Emergency Communications Program Manager
        sbrown@imd.idaho.gov
    d. Once the signed form is received, please email it to ipaws@fema.gov.

Appendix C: Missing Person Alert Activations

Alert	Activation
AMBER	The Idaho AMBER Alert Portal Activation is a form filled through the ILETS CPI OpenFox system to all qualified Idaho Law Enforcement agencies that have a terminal to request an ALERT using the EMP mask. Please see ILETS training for information on how to request alert. Once the request form has been filled out, follow up with a phone call to ISP RCC's to request an AMBER Alert (North Idaho 208-209-8730; South Idaho 208-846-7500).
BLU	To request a BLU alert, send an email to mpalerts@isp.idaho.gov and follow up with a phone call to ISP RCC's (North Idaho 208-209-8730 or South Idaho 208-846-7500)
Missing and Endangered Person(s) (MEP)	Endangered Missing Person alerts must be for someone whose disappearance includes, but is not limited to the following situations: 1.Being incapable of returning to the missing individual's residence without assistance by reason of: 2. Mental illness 3. Intellectual disability 4. Dementia 5. Weather conditions 6. Another physical or mental incapacity that requires care of the individual or management of the individual's property; (ii) Someone who is missing as the result of abduction by a stranger and does not meet the criteria for an AMBER alert or BLU alert; (iii) Someone who is missing under unexplained, involuntary, or suspicious circumstances; (iv) Someone whose disappearance may be the result of the commission of a crime; (v) Someone whose disappearance occurred under circumstances that are inherently dangerous; (vi) Someone who needs medical attention or prescription medication; or (vii) Someone who has previously been the victim of a threat of violence or an act of violence. To request an alert, please email mpalerts@isp.idaho.gov and follow up with a phone call to ISP RCC's (North Idaho 208-209-8730 or South Idaho 208-846-7500)

Appendix D: Alert Origination Software Providers

Alert Origination Software Providers (AOSP) with IPAWS capabilities
Alerts Sense/Konexus
Alertus Technologies
Asher Group – Hyper Reach
ATI Systems – MassAlert
Blackberry – AtHoc IWS
Buffalo Computer Graphics – DisasterLAN
CivicReady
Comlabs- EMNet
Desktop Alert
Everbridge
Genasys
GSSNet - Alert Studio
HipLink
HQE Systems – SiRcom SMART Alert
Information Logistics – IRIS/HELP
Inspiron Logistics WENS
Juvare - WebEOC
KDEE Technology LLC – On-The-Go Alerting
Monroe Electronics – DAS-EOC
Motorola Solutions – CommandCentral Notify
Nixle
On Solve - CodeRED
Rave Mobile Safety
Regroup Mass Notifications
Singlewire – InformaCast
Swift Reach – Swift911
Titan HST