



In Control: A Guide to Navigating Emergency Alerting With Authority and Precision

How to Stop Hesitating and Learn to Use
IPAWS With Confidence

By OnSolve in collaboration with Eddie Bertola and Peter Gaynor

Table of Contents

Introduction	4
The Mindset Shift: Sending With Confidence	6
Mission Critical Knowledge	6
<i>What Might Go Wrong?</i>	6
<i>The Paradigm Shift</i>	8
Understanding IPAWS	9
Mission Critical Knowledge	9
<i>Official Alerts Versus IPAWS Alerting</i>	9
<i>The 3 IPAWS Alert Pathways</i>	10
<i>Your State Emergency Alert System (EAS) Plan</i>	12
<i>Understanding Your State EAS Backbone and Front End</i>	13
Continuing Education	14
<i>Advanced Tips: The 3 IPAWS Alert Pathways</i>	14
<i>Test Codes</i>	15
<i>Deep Dive: Your State Emergency Alert System (EAS) Plan</i>	16
<i>National Public Warning System (NPWS)</i>	17
<i>Recommended Reading</i>	17
Foundation of an Emergency Alerting Program	18
Mission Critical Knowledge	18
<i>Ownership</i>	18
<i>Program Overview</i>	19
<i>The Unintended IPAWS User</i>	20
Continuing Education	20
<i>Additional Tips for Your IPAWS User Policy</i>	20
<i>EMAP Accreditation</i>	21
<i>Recommended Reading</i>	21

Table of Contents

Training, Education & Maintenance	22
Mission Critical Knowledge	22
<i>Procedural and Technical Training</i>	22
<i>Drills and Exercises</i>	24
<i>People Drills</i>	24
<i>Technical Drills</i>	25
Continuing Education	26
<i>Public Education</i>	26
<i>Additional Resources</i>	26
Continuous Improvement	27
Mission Critical Knowledge	27
<i>After-Action Reports (AARs)</i>	27
<i>Analytics/Record Keeping</i>	28
Continuing Education	28
<i>Additional Resources</i>	28
Message Creation	29
Mission Critical Knowledge	29
<i>Coordinate Locally</i>	30
<i>Alerts Should Be Community-Driven</i>	30
<i>Have Message Templates Ready & Be Clear</i>	30
<i>Leverage Technology</i>	30
<i>The Warning Lexicon and Message Design Dashboard</i>	31
Continuing Education	33
<i>Additional Message Creation Tips</i>	33
Press “Send”: Your Confidence Checklist	34
Conclusion: The Big Question	37
About the Authors	38
About OnSolve CodeRED	38

Introduction

By Peter Gaynor, Vice President, Resiliency and Disaster Recovery, Hill International



Every year, [approximately 7,000 Wireless Emergency Alerts](#) (WEAs) are issued by federal, state and local governments, as well as tribes and territories. These alerts cover a wide range of hazards, from weather warnings and watches to AMBER Alerts. However, they all come through a single platform: The Federal Emergency Management Agency's (FEMA) Integrated Public Alert and Warning System (IPAWS).

Emergency managers have two main goals when a disaster strikes:

- 1 Protect lives.
- 2 Minimize property damage.

There are three things emergency managers must do in order to accomplish these goals:

- 1 Craft clear, precise communications that tell those in danger exactly what to do.
- 2 Send the message at the right time.
- 3 Have an effective way to distribute the information.

There have been a growing number of instances where lifesaving WEA messages were never sent or were sent late. The Lahaina, Maui tragedy is the most recent in a string of “it didn't have to be this way” events. When emergency officials don't issue an alert soon enough or not at all, the repercussions can be severe — resulting in more lives lost and more damage to communities.

We have come a long way in building a technologically reliable national alert and warning system. However, we have failed in the soft skills needed to ensure those charged with pushing the “send message” button have the appropriate level of confidence that their action will result in a positive outcome.

More simply stated:

There are some that are reluctant or afraid to push the send button because they fear the consequences of a wrong decision. The main causes of fear are:

- Stress
- Liability concerns
- General confusion
- Budget/Cost concerns
- Lack of training and practice
- The unknown (What will happen if I press it?)
- Prior negative experience(s)

The solution is simple:

To improve confidence, you must improve competence. This involves creating muscle memory, gathering knowledge of the alerting ecosystem, conducting effective training and adopting a mindset shift. Competency creates a sense of self-assurance, especially during those defining moments when you need to send an emergency alert.

How To Use This Resource

This guide is designed to increase the confidence of those charged with pushing the send button. It is not meant to be an exhaustive treatise on emergency alerting. Rather, it is a concise handbook that provides tips, tools and tactics to help emergency managers confidently press the send button when it counts the most.

Most of the sections in this guide are divided into two sections:

- 1 Mission Critical Knowledge:** The essential information everyone should know. The details provided here should be bookmarked so you can reference them as needed during an emergency.
- 2 Continuing Education:** The supplemental information here is a great resource for certain roles and job functions on your team that require a deeper understanding of the entire emergency alerting process.

The guide also includes a checklist you can use to make sure you have all of the critical steps in all of the phases of the emergency alerting process covered. Feel free to hang up physical copies of this checklist for your entire team to use.



The Mindset Shift: Sending With Confidence



Mission Critical Knowledge

A comprehensive and up-to-date program and regular training will help alleviate the apprehension around how to use the IPAWS emergency alerting system. But we still need to shift our mindset to fully overcome the fear and actually press “send.”

What Might Go Wrong?

Often, those with the authority to send an emergency alert waste precious time thinking about what might go wrong.

As the clock is ticking, officials often ask themselves:

- What if I make the situation worse?
- What if I set something in motion that unnecessarily drains resources?
- What if I get fired?

These fears often result in officials continuing to go up the chain of command, asking for permission to launch an alert. The result? Paralysis — The alert goes out too late or not at all, causing more lives to be lost and more property to be damaged.

Potential issues include:



Lack of Information

This becomes an issue when an alerting authority sends out an alert, warning or notification with only certain pieces of the puzzle. This can easily turn into a “The sky is falling!” situation. When the community reads the message, it only contains enough information for people to become scared and/or confused. Neither one of these emotions leads to good decision making and will generally not empower the community to act in the way you intended them to act.

There are two best practices to help avoid this issue:

- 1 Have someone who doesn't have all of the inside information review the message to identify missing details you may be assuming others know.
- 2 Make sure you include all of the parts of a complete message (which we cover later in this guide). From a high level, however, this can be accomplished by using the Message Design Dashboard to train before an incident and even during the crafting of the specific message during the incident. It doesn't take much more effort and will provide the community with the best possible message.



Incorrect Information

Even if you include all the components of a complete message, sometimes the information is just incorrect. In the heat of the moment, it's important to take a few extra seconds to double check the information. This can be as simple as checking the spelling of streets, cities and names of those involved. If you're using a hyperlink, make sure it's written correctly, and it works. You may think this is an unnecessary step, but unfortunately this does happen, and the community ends up clicking on a link that doesn't provide them anything but frustration.



Too Wide of an Activation Area

Activation Areas are not a one-size-fits-all approach. You should not always presume to extend your activation reach to the outer boundaries of your jurisdiction. Continue to weigh the balance of alerting fatigue with the current needs of the situation. Base the activation area on actual information from the investigation or situation rather than what you always do.

Keep records on the size of activation areas and the impact it has on the community and the outcome on the case. Follow the information instead of past practices. There are times when it's possible to focus on a smaller activation area and still address the issue and help those in need without causing alarm in a wider area.



Lack of Training

You can't escape training. You may postpone it, but it will happen. There is pre-event training and on-the-job training. The goal is to get as much of the pre-event training as possible because the on-the-job training often comes at a much higher cost to your time, money and well-being.

There are those that have deep scars from tragic experiences resulting from on-the-job training. If you ask them, they will tell you they wished they could go back and better prepare themselves for these incidents.

While you can't account for every variable in an emergency situation, you can and should account for yourself, your training and your preparation to respond to a call you receive. The 'What if?' game is dangerous enough without you having to think back and know you could have applied an alerting tool differently if you only knew then what you learned after the emergency incident.

The Paradigm Shift

In this business we live with risk every day. It's impossible to eliminate it. Our job is to minimize risk to an acceptable level. The overarching goal is action. Taking a positive action (even if it's not perfect) that protects life and minimizes property damage in a timely manner is our ultimate goal.

Emergency officials need to shift their mindset and accept they will not always be perfect. Mistakes WILL happen. Emergencies are low frequency/high risk situations. The stress level is high, and in the heat of the moment, the alert may contain a misspelling or lack a piece of information. And that's okay.

Every mistake is a chance to hone your skills and make the process better the next time by asking:

What can we do differently?

We need to stop fearing mistakes and instead fear inaction.

Officials who have been through an emergency and didn't launch an alert quickly can tell you they do not want to be in that situation again. It is in your best interest to take action and press "send!"

Think about what will happen if you take NO ACTION (loss of life) compared to what will happen by taking positive ACTION (lives saved). Most of us would rather be found guilty of taking too much action as opposed to being found guilty for doing too little (or nothing at all).



Understanding IPAWS



Mission Critical Knowledge

[IPAWS](#) is “FEMA’s national system for local alerting. It gives federal, state, local, tribal, and territorial public safety agencies the ability to send WEAs, EAS alerts, weather and non-weather-related emergency messages simultaneously through NOAA weather radios, and alerts through systems like sirens and digital billboards.” It’s one of the most powerful tools to help government officials keep their communities informed and safe.

A thorough understanding of IPAWS is an essential element for making the right decision to send an alert.

Through IPAWS, local alerting authorities can send out their own targeted emergency alerts to make sure only impacted individuals receive the message.

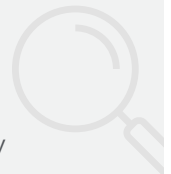
Official Alerts Versus IPAWS Alerting

Official alerts exist in every state, and they’re becoming more and more common. The AMBER Alert, Silver Alert, Blue Alert, Gold Alert, Golden Alert, Purple Alert and Feather Alert are a few examples. There are dozens more.

Each of these alerts are designed to accomplish a specific task with a dedicated process and resources. One of the common misconceptions is that these alerts and IPAWS are the same. IPAWS is the keeper and developer of tools of alerting and although mentioned in each of the above examples of official alerts, it is not tied down or restricted to being used in only official alerting. Alerting authorities have the authority to send alerts, warnings and notifications outside of official alerting as they deem appropriate.

Real-world scenario

A missing 6-year-old girl with a cognitive impairment ran away from a park and has not been located. Nightfall and freezing temperatures are approaching and the exigency for her recovery is extremely high. The alerting authority may be restricted by legislative regulations to not call this an AMBER Alert because there is no sign of an abduction. However, the need to immediately find her still exists. There are no Federal restrictions limiting IPAWS alerting by the local jurisdiction in this situation, even if it is not an official alert.



Opt-in Alerting

Opt-in alerting occurs when community members sign up for alerts through an application. This is an internal alerting function and does not interact with IPAWS. Opt-in alerting has potential additional capabilities to send pictures, maps and videos. IPAWS does not have those capabilities.

Opt-out Alerting

IPAWS messaging is an opt-out system that presumes everyone in the activation area needs the information. If a person does not want the information, they can opt out. It has limited capabilities. It is text only and cannot send pictures, maps or videos.

The 3 IPAWS Alert Pathways

1 Emergency Alert System (EAS)

- These messages are mostly for television and radio broadcast transmission.
- They can be delivered in two languages. English is required. Spanish is optional. A single message can include both English and Spanish at the same time, but only one language is delivered once depending upon the device settings.
- For both radio and TV, the message should contain no more than 1,600 characters per the Federal Communications Commission, although IPAWS does not currently validate or limit this character limit. However, a future release of IPAWS will likely enforce this restriction.
- There are four ways to include an audio “mimetype” in an EAS message. (*Note: See Continuing Education for specifics.*) If broadcast content exceeds two minutes playing time it may be truncated by exchange partners except for Presidential Messages.
- For TV, as the audio announcement plays, the written message will also crawl across the screen, typically twice. However, there may be some variation since broadcast stations are all voluntary and have different capabilities.
- During live IPAWS testing, use one of the following event codes: Required Weekly Test (RWT), Required Monthly Test (RMT) or Practice/Demo (DMO). It is very important to use the correct codes when testing because all sent messages are processed. So even test messages will be transmitted, but the receivers will know not to continue the distribution based on the test codes.

2 Wireless Emergency Alert (WEA)

- These messages are sent to cell phones and other WEA capable devices via push broadcast through cellular service towers. Push broadcasts will still be delivered even when regular text messages and phone calls over wireless devices are jammed.
- Per the FCC, [97 percent of households](#) in the U.S. have a WEA capable device.

- Messages in English are required. Spanish is optional. Alerting Officials (AOs) can and should send Common Alerting Protocol (CAP) messages in both languages. Only one language is delivered to the user depending on the hardware settings. AOs can include as many “info” blocks as they want, but only the first English and first Spanish block will be transmitted.
- Ninety characters is mandatory, while 360 characters is optional, included in a single message. Only one message is displayed depending on the user device capabilities (i.e., WEA 1.0, WEA 2.0 or WEA 3.). A message with more than 90 or 360 characters will be rejected.
- Certain special characters may count as more than one character. Embedded URLs and links also count toward the character count.
- The best practice is to use 360 characters to create an effective message, but it must include the required 90-character CMAM text. If you have the capabilities to also send a Spanish language message, you should do it too.
- If a message includes any of the following special characters, it will be rejected: “{”, “}”, “|”, “\”, “^”, “~”, “[”, “]”.
- Attachments are not allowed with a CAP message. However, AOs can embed links into the CMAM text. Hyperlinks are not vetted or verified for accuracy or uptime.
- Delivery is based on the recipient’s geographic location (proximity to a cell tower). The cellular providers determine when and where notifications are received, so make sure to contact those providers to determine range distribution and geographic overlap parameters. Each provider has different policies for WEA.
- Federal Information Processing Standards (FIPS) is always required. A polygon or circle is optional. A message without a FIPS (geocode) and Area Description will be rejected. FIPS code and polygon use must match the AO permissions. If a polygon is included, it must include less than 10 shapes or 100 total nodes.
- “Cancel” will stop an active push broadcast.
- “Update” will cancel an active alert and send a new one.

3 NOAA Weather Radio (NWR — Formerly known as NWEM)

- These messages run on radio frequencies outside the normal AM or FM broadcast bands.
- Agencies should not include supplementary audio clips.
- Messages are required in English. Spanish is optional, but it is ignored.
- Your WFO will review and edit each message to conform to the National Oceanic and Atmospheric Administration (NOAA) text-to-speech standards. Therefore, these alerts will be delayed until that process is completed by human interaction.

- To enable NWR broadcast, the National Weather Service (NWS) must first generate a World Meteorological Organization (WMO) teletype style formatted version of the alert and transmit it to NWS offices via the NOAAPORT. NOAAPORT is also monitored by many third parties who may also redistribute the alert.
- Correct population of the “senderName” element is important because NWS populates the alert text broadcast over NWR and other NWS dissemination systems with information from the “senderName” element. This is done to ensure proper attribution and clarity in the alert message. NWS makes a clear distinction between the alerting authority generating the alert and the alerting authority requesting the alert, which are not always the same.
- NWR does not accept circles and limits polygons to 20 nodes.
- Updates are not handled as emergencies. The best practice is to update the original message to stop the retransmission of the original.

The owner of the program should regularly check FEMA's site for [monthly information tips](#) for changes to the pathways, update documentation and educate all users accordingly.

Your State Emergency Alert System (EAS) Plan

The Emergency Alert System (EAS) is a national public warning system that requires TV and radio broadcasters to offer the President the communications capability to address the American public during a national emergency. The system also may be used by state and local authorities to deliver important emergency information such as AMBER (missing children) alerts and emergency weather information targeted to a specific area.

The EAS plan allows authorized authorities to promptly distribute important local emergency information. Being an emergency manager overseeing the initiation of alerts in your local, county, tribal, territory or state is crucial for ensuring that the EAS plan aligns with the community's requirements.



Understanding Your State EAS Backbone and Front End

Emergency officials need to understand how the systems within their state are connected. Technology changes quickly, so officials also need to remain aware of updates. All documentation should reflect changes, and the information pertaining to changes should be distributed to all individuals involved in the alert process.

Everyone involved in launching alerts also needs to be familiar with the front end of the system, including the required codes and protections in place. One example of a front end that's used by more than half of IPAWS alerting authorities is OnSolve CodeRED. It gives government agencies the ability to quickly and easily deploy IPAWS alerts during emergency situations.

Comfort and familiarity with the front end and how all systems are connected in your region is essential for building confidence during a crisis.

Mindset Shift Reminder!

Every second counts during an emergency. A solid understanding of IPAWS removes the guesswork and builds confidence. The incidents below are just a few examples of “It Didn’t Have to Be This Way” moments. Let these serve as lessons in the importance of sending rapid, accurate and targeted alerts.

Ask yourself: What can we learn from past mistakes?

Maui Wildfire: By the time the county sent an emergency cellphone alert at 4:16 p.m., the fire had already been spreading through town. The alert did not cover all areas to which the wildfire soon spread. Death toll of at least 100 people.

2021 Winter Storm Uri in Texas: 246 people died. Reports of a “lack of coordination in disseminating messages to the public.”

Continuing Education

Advanced Tips: The 3 IPAWS Alert Pathways

1 Emergency Alert System (EAS)

- The four ways to include an audio “mimetype” in an EAS message are:
 - “audio/x-ipaws-audio-mp3”
 - “audio/x-ipaws-streaming-audio”
 - video/x-ipaws-video”
 - “video/x-ipaws-streaming-video”
- An error code is returned if the <url> element includes:
 - A missing http:// or https://
 - A missing period
 - A space
 - A “?”
 - A length exceeding 2,083 characters
- Only use FIPS codes. EAS does not recognize polygons.
- FIPS codes and Event codes are monitored by your Local Primary 1 (LPI) broadcasters. These are the lead stations in the alerting system.
- Your launch to IPAWS is not complete until you go back to your broadcasters and verify they’re monitoring for your FIPS codes and Event codes. Do NOT assume the LPI will automatically do so.

2 Wireless Emergency Alert (WEA)

- Polygons and Geographic Information System (GIS) overlays are restricted to 100 nodes.
- For live IPAWS testing, use Demonstration Message (DMO) handling code only.

3 NOAA Weather Radio (NWEM)

- You can identify a Requesting Agency for NWEM.
- Use FIPS codes only. NWEM does not integrate with maps at this time.
- For testing codes, check with your local WFO.



Test Codes

FEMA's [IPAWS Best Practices Guide](#) provides important details about the three test codes available for the various IPAWS Alert Pathways. Some of the most important details are included below, but it is recommended to refer to the IPAWS guide for additional information.



RMT — Required Monthly Test for EAS & WEA

- Typically prescheduled and coordinated state- or region-wide on an annual basis.
- Generally originate from a pre-designated local or state primary station or a state emergency management agency.
- Broadcast stations and cable channels must relay RMTs.
- They must be conducted between 8:30 a.m. and local sunset during odd numbered months, and between local sunset and 8:30 a.m. during even numbered months.
- Received monthly, tests must be retransmitted within 60 minutes of receipt.
- An RMT should not be scheduled or conducted during an event of great importance.
- Although RMT is available for WEA, it is not recommended for live testing. Rather, using RWT for WEA testing is the best option to avoid having to obtain an FCC Waiver.



RWT — Required Weekly Test for EAS & WEA

- A test message that consists, at a minimum, of the header and end of message tones.
- RWTs are scheduled by the station on random days and times during weeks when there is no Required Monthly Test scheduled.
- Broadcast and cable operators generally do not relay incoming RWTs.
- EAS RWTs may originate from state and local alerting authorities to confirm the operational status of their IPAWS live alerting software configuration without interrupting broadcast or cable programming.
- Use RWT instead of RMT if the agency does not plan to interrupt the public.
- An FCC waiver is not needed when using test event codes for WEA. A waiver IS required to send live tests — using Event Codes other than RWT — to the public.
- Do NOT test WEA on a weekly basis. RWT is an Event Code type, not a mandate.
- Do not use Required Monthly Test (RMT) to conduct WEA tests because an RMT message will activate broadcast equipment and disrupt broadcasters' monthly test schedules if EAS distribution is accidentally selected.
- WEA tests will only be received on cellular devices that have opted to receive WEA test alerts.



DMO — Practice/Demonstration Warning for EAS, WEA, & NWEM

- A DMO is a demonstration or test message used for purposes established in state, including local, tribal, or territorial EAS plans.
- NWEM does not support event codes RWT and RMT. Use DMO for testing NWEM.
- DMO can be used by authorized officials to test their NWEM capabilities or siren systems.
- Use RWT instead of DMO to test EAS/WEA and avoid disrupting the public.

Deep Dive: Your State Emergency Alert System (EAS) Plan

The EAS plan provides guidelines for broadcasters, cable operators and all other EAS participants to determine:

- Mandated and optional monitoring assignments
- EAS codes to be used
- Guidance for message originators
- Other additional elements of the EAS which are unique to the state

A designated emergency manager can use the EAS to broadcast a warning from one or more major radio stations in a particular state. EAS equipment in other radio and television stations, as well as in cable television systems in that state, can automatically monitor and rebroadcast the warning.

Emphasizing the significance of these plans is essential to guaranteeing the proper transmission of emergency messages through EAS alerts to all intended recipients. This ensures that pertinent information reaches the public members who need to be informed about the triggering emergency situation.





National Public Warning System (NPWS)

The National Public Warning System (NPWS) are radio broadcast stations located throughout the country with a direct connection to FEMA and strong transmission capabilities. Also known as Primary Entry Point (PEP) stations, they send emergency alert and warning information before, during and after an emergency or disaster.

The FEMA NPWS is the main source of initial broadcast for a national alert, and the NPWS can reach more than 90 percent of the U.S. population thanks to an increased number of PEP facilities.

While many officials may be unfamiliar with PEP stations, they're an important resource for continuity of government. Recent modernization began with the adoption of a new digital standard for distributing alert messages to broadcasters.

Pro Tip

NPWS stations are equipped with back-up communications equipment and power generators designed to enable them to continue broadcasting information to the public during and after an event. If you haven't visited a PEP site listed in your State EAS Plan you should make a point to do so immediately to better understand its full capabilities.



Recommended Reading

[FEMA — IPAWS Best Practices: Integrated Public Alerting & Warning System \(IPAWS\) Guidance and Techniques for Sending Successful Alerts, Warnings, and Notifications](#)

Foundation of an Emergency Alerting Program



Mission Critical Knowledge

Ownership

An effective emergency management program is the first step in overcoming fear and building confidence. Ownership has to come from the top. The person responsible for launching an alert (whether that be the state or local director of emergency management) should personally own the program.

Why? Because they're the individual who is ultimately responsible and whose job is on the line should an alert fail to go out. Delegating this responsibility away is a recipe for disaster.

Mindset Shift Reminder!

Too often, time is wasted while officials ask the next person in command for permission to launch an alert. The truth is each person in the chain of command should feel empowered to press "send." Permission to act without orders should be documented in your formal policies and procedures.

Ask yourself: What's at stake with each second that goes by deliberating over whether to press the button?

Program Overview

The program must be detailed and comprehensive.

Start by creating an IPAWS user policy to make procedures crystal clear and verify all personnel review it. Such a plan provides the teeth and the empowerment for using alerts. It also takes the guesswork out of the process, instilling confidence.

We often worry about the unexpected and forget to plan for the events we should expect. If your community is prone to hurricanes or tornadoes, for example, these expected events should be covered in detail in your emergency response program.

It's also important to remember that managing the system and pressing "send" aren't the same thing. There are technicians who manage and maintain the system, and then there are the decision-makers. The person who owns the program cannot assume that everyone knows everything.

It's imperative to ensure that everyone on the roster that has the authority to launch knows the codes, knows the passwords and knows every step involved in the process to launch an alert.

To create your policy, start by asking the right questions:

The Who, What, Where, When, How

- **Who** — Who has the authority to initiate an alert in your agency? Who are the backups for these individuals? Who are the alert recipients?
- **What** — What is the content you want to send? What action do you want your recipients to take?
- **Where** — Where do you want the alert to reach? (i.e., the technical reach of the broadcasters, TV and radio, or cellular.)
- **When** — When do you use IPAWS to send an alert, and what are your agency's guidelines?
- **How** — How do you use IPAWS? — Do you know the difference between the three delivery methods of IPAWS? EAS, WEA and NWEM (each is different from the alert creation to the way in which they are delivered).

And remember, the real work comes with maintaining the program over time. As the technology used to send alerts changes, it's critical to revisit the program and update it accordingly. Turnover is also an issue, especially at the local level. Replacements need to be identified, documented and trained immediately.

The Unintended IPAWS User

There will be a day when the written procedures, training, drills and exercises will not be enough. When the people you have invested all your time and energy to ensure you can launch an emergency message are unavailable. Now what?

Let's discuss some of the possible workarounds.

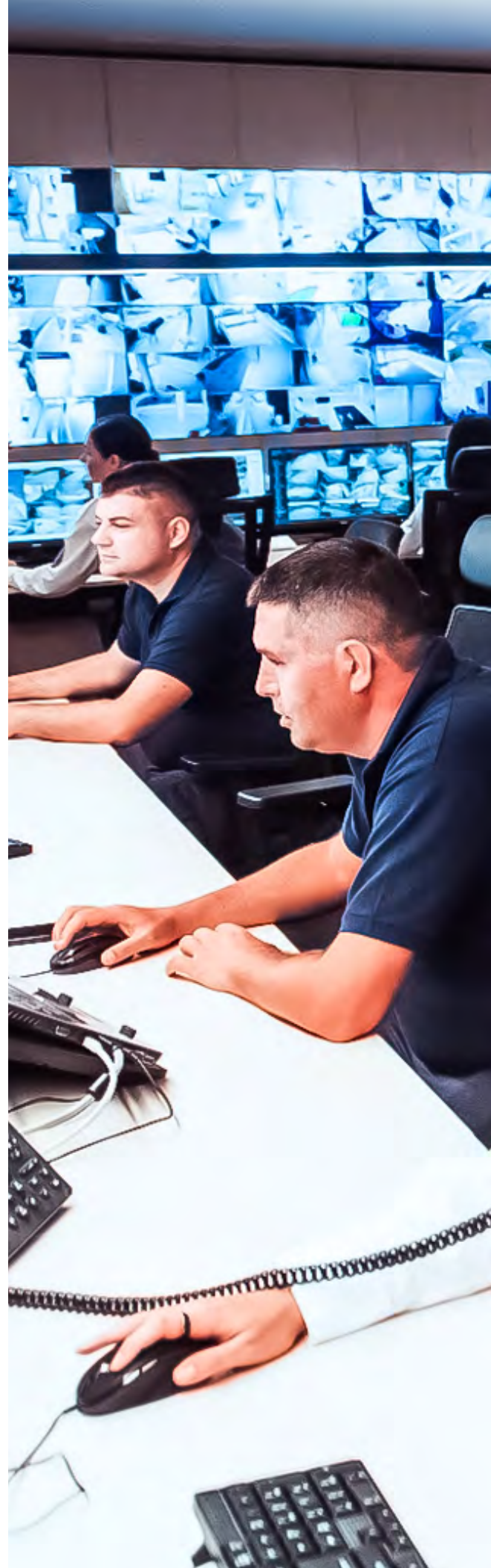
- 1 First, ensure your entire staff, from the director down to the most junior employee, understands the IPAWS/WEA system and the critical importance of timely and accurate emergency messages.
- 2 Second, consider a wide range of back-up options. If you're at the local level, can the county or state launch on your behalf? If you're at the state level, can another state or the FEMA Operations Center launch on your behalf?

The bottom line is you must have a failsafe because lives and property are at stake. As an emergency manager, it is one of the most important actions you will take (or fail to take).

Continuing Education

Additional Tips for Your IPAWS User Policy

- Keep your plan as short as possible. You should be able to reference the plan at a moment's notice without wading through an encyclopedia-sized book.
- Check with your local broadcasters to see who receives the alerts and how far the alerts reach.
- Don't forget to include password management in your documentation. Hint: A post-it note on someone's computer screen is not effective password management.



Pro Tip

Give each authorized launcher their individual passwords and launch codes. Direct those authorized users to store the passwords on their cell phones. If you're a CodeRED user, you can even have a backup plan where the authorized launchers can provide a PIN to the CodeRED 24/7 help desk, and they can launch on your behalf.

EMAP Accreditation

- EMAP accreditation is one way to ensure your emergency management program is comprehensive and effective. It also increases confidence and reduces fear. [EMAP](#) is an independent non-profit organization. Its mission is to “foster excellence and accountability in emergency management programs, by establishing credible standards applied in a peer review accreditation process.”
- Accreditation is voluntary. However, some states have tied accreditation to EMPG funding. Accreditation also shows that a program meets national standards.
- In the 73 standards outlined in the latest ANSI/EMAP 5-2022 Emergency Management Standard, Section 4.7 Communications and Warning provides an excellent foundation for building your program on solid ground.
- The standard outlines five key components:
 - A program that includes hazards outlined in your jurisdiction's Hazard Identification Risk Assessment (HIRA) plan.
 - A communications, notification and alert and warning system(s) that supports the HIRA, has backup systems, can operate in any environment and that is tested on a regular basis.
 - Written operational procedures for each of the systems.
 - Ensuring that the systems are interoperable.
 - A maintenance process for plans identified in the standard which includes a method and schedule for evaluation and revision.



Recommended Reading

[Emergency Management Standard: Emergency Management Accreditation Program, EMAP EMS 5-2022](#)

Training, Education & Maintenance



Mission Critical Knowledge

Procedural and Technical Training

IPAWS is like any other lifesaving equipment. The first time you use it should not be during an emergency. Lack of a process leads to poor decisions. Consistent and regular training and education creates the muscle memory needed to quickly launch an alert during an emergency. Just like with program ownership, training starts at the top. The person ultimately in charge must know exactly how the system works.

FEMA requires a two-hour online course for the people who send out alerts. Much of it is focused on the technical aspects of alerting rather than the decision-making process. Additionally, one-time training is not enough. Formal training should be scheduled at least once a month so everyone involved is extremely familiar and comfortable with the system.

To ensure a higher level of confidence, you should also plan for random, unannounced drills and tests on a regular basis. The frequency of pop-up drills should be determined by success and confidence. If your team is hesitant about the procedures to follow or how to launch an alert, then random drills should be held more frequently until they're navigated with assurance.

Training needs to include EVERY aspect of the launch sequence and should cover multiple scenarios, including, but not limited to, the following:

- The decision to launch has already been made by the designated decision maker and the operational team is just routinely following instructions to launch.
- A meeting is required to discuss the details of the launch such as drafting a message and determining geographic boundaries.
- An emergency occurs after hours, and the designated decision maker is unavailable to make a decision. In this situation, who is next in line to give authorization? Can that person launch the alert from home? Do they have a copy of the written procedures and passwords with them to launch the alert remotely?

Training through various scenarios builds confidence among your entire staff so they can still respond appropriately and swiftly when something out of the ordinary happens — because it will.

A comprehensive training program should also cover such items as:

- Written launch procedures
- Passwords/Codes required
- Trigger circumstances
- Alert creation (including specifics on message content and character limit)
- Discussion and decision on the geographic activation area
- Discussion and decision on which tools to use
- Access and functional needs within the community
- Alert launch (including how to send it and when to send it)
- Recipient list/Geographic parameters
- Acknowledgement of any errors or barriers in the process

Even basic items like making sure the system is plugged in and software updates should be part of training to avoid simple mistakes during an emergency.



Mindset Shift Reminder!

There is no substitute for regular and frequent training. Case in point: The Lahaina wildfires weren't the first time Hawaii had issues with its emergency alerting system. In 2018, the state infamously [sent out a false warning of an incoming ballistic missile](#), resulting in a federal recommendation that emergency management agencies conduct regular internal drills to maintain proficiency on the tools.

Ask yourself: Are training and drills conducted regularly to instill a sense of confidence in my team's ability to create and send an alert during various types of emergency scenarios?

Drills and Exercises

In addition to regular training, emergency officials also need to conduct drills and exercises on a regular basis. This is the only way to keep the system “warm” and ensure everyone feels ready to respond during a crisis — even if it’s in the middle of the night.

When it comes to ensuring you can efficiently perform the critical tasks of sending an emergency alert there are two elements you must focus on: People drills and technical drills. They are connected but they are not the same.

People Drills

Without people who have been trained to the written standard you will struggle to send prompt, timely and accurate emergency alerts. Training needs to be progressive, experiential and frequent (very frequent). Periodic testing should be conducted for all users to stay fresh and up to date on the three IPAWS alert pathways.

Program owners should also conduct monthly proficiency drills with staff, dispatchers and anyone else involved in launching IPAWS messages. Rehearsals should be conducted exclusively in the IPAWS test environment, but they should be realistic and follow the parameters for each alert pathway. Practice using the codes and writing messages within the prescribed character limits. Too often, tests are conducted using real-world language or in the LIVE environment just stating, “This is a test.”

When assessing the effectiveness of your people drills, ask yourself the following questions:

- Have the individuals who are designated and authorized to send emergency alerts familiar with the written procedures?
- Have they reviewed the procedures step by step, both with oversight and on their own?
- Have they been given the opportunity to conduct a “live” training by launching WEA tests using the Required Weekly Test (RWT) code?
- Have they sent emergency alerts and warning messages from the alternate or back-up location?
- Have they conducted a no-notice drill during work hours and after work hours? From their homes?
- Have you told the authorized individuals what they need to do if they cannot obtain your permission to launch during an emergency?
- Do they have authority to act in the absence of orders?

The bottom line is you can’t leave anything to chance — even the obvious.

And remember, it’s a process. The technology is always changing, so training and education never stop. Fortunately, some emergency alerting systems provide a test environment, which makes it easier to stay current on the latest technological changes.



Technical Drills

In most emergency management organizations, there are communication and IT technicians responsible for the maintenance and sustainability of communication, alert, warning and notification equipment. Even though these technicians may never launch an emergency alert, failure to include them in your SOP can leave your team unable to send an emergency alert due to technical issues.

As a part of these drills and exercises, the technical team should:

- Conduct technical and functional training and tests of the hardware.
- Ensure software and firmware on all equipment and user front-end interfaces are up to date.
- Perform maintenance at all alternate sites capable of launching emergency alerts.
- Test back-up emergency power on primary and alternate launch sites.
- Set up and test redundant internet access with multiple ISP providers.
- Regularly test launch capability from mobile sites (e.g., wheeled command post or emergency operations center).
- Confirm all designated and authorized individuals are aware of any and all password updates.

The important task of sending an emergency alert message requires organizations to implement vigorous oversight and focus on the people and technical aspects of emergency alerts. Without an integrated and complementary approach, successful emergency alerts become daunting.

Continuing Education

Public Education

IPAWS is working on developing updated public education. The current guidance is for local alerting authorities to reach out to their media partners and look for ways to educate their communities via local media, social media and community events. There are some limited [PSA](#) and educational resources available on the FEMA website.

In general, outreach should educate the public on:

- What is IPAWS
- The different mechanisms of outreach from the IPAWS system
- What they can expect from their jurisdiction
- What they will be alerted about
- What they should expect to see in an alert

A list of FAQs to the most common questions around emergency alerting increases public confidence in your agency's ability to keep the community safe. It also ensures residents will know what to expect from an alert and helps prevent the worst-case scenario — residents opt out of receiving potentially life-saving alerts.

Additional Resources

[IPAWS Program Planning Toolkit](#): This resource guides alerting authorities through the process of collecting and organizing their disaster protocols. After a form has been completed, the system generates a simple, editable document that can be shared with response officials and easily referenced when an immediate response is needed. It also includes prewritten templates for various emergencies and a message generator that uses social science to craft alerts.

Continuous Improvement



Mission Critical Knowledge

Mindset Shift Reminder!

Consider the following scenario: A wildfire is spreading through your community. Cell towers are burning while officials delay looking for passwords or remembering how to use the system or deciding the geographic parameters or whether to send an alert at all. By the time the alert is sent, the fire has eaten up the infrastructure and not everyone receives the alert.

These types of issues can be avoided by building confidence (and competence) through constant improvement.

Ask yourself: What actions is my team taking to continue to build comfort with the steps involved in sending emergency alerts? What else can we be doing?

After-Action Reports (AARs)

AARs are an essential and required component of emergency alerting. The data captured should be used to improve your program, policies and procedures so you can put a plan in place to respond more effectively during the next emergency.

An AAR should answer questions like:

- Did the designated emergency officials take the appropriate actions?
- Was an alert launched in a timely manner?
- Was the alert missing critical information?

The report should also include a summary of the incident and the actions taken, as well as a section that outlines recommendations for future improvement.

Analytics/Record Keeping

To utilize actionable intelligence from all three alert pathways, ensure you're preserving data for analysis. All outcomes should be tracked and recorded to create statistics to serve as a basis for recommendations as new cases develop. This includes, but is not limited to, the details of search and rescue missions, such as the average length of time to locate missing persons and average geographic span of search grids in cases of successful recovery.

It's also essential to perform regular maintenance on your emergency alerting system. A logbook of all actions taken serves as an official record of the actions you decided to take should you ever be questioned. It also demonstrates your commitment to the emergency alerting program.

The logbook should include the following details:

- Record (including date and time) of software updates
- Names of individuals who performed the updates
- Verification that functionality was tested after an update was installed
- Dates of training and drills and a list of attendees/participants
- Results of training exercises and drills

Continuing Education

Additional Resources

[FEMA Preparedness Toolkit – Templates and Resources](#): This site provides a variety of templates, tools and other resources designed with continuous improvement in mind. Users can search by categories and tags. An AAR template is available here for those in need.

Message Creation



Mission Critical Knowledge

Fear of pressing “send” often stems from worrying about whether your alert is accurate and effective. Alerts should be written for someone who doesn’t know what’s going on in order to avoid ineffective alerts. Recipients can be paralyzed if they receive enough information to worry, but not enough information about what actions they should take.

These best practices can help officials create clear and concise messages that mitigate the impact of an emergency.

Mindset Shift Reminder!

Jeanette Sutton, Associate Professor in the College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University at Albany, SUNY, specializes in emergency alerts. [She admits](#), “there is little guidance for agencies on how to formulate the alerts, so they can sometimes go out with missing information (no location identified) or incorrect information or confusing instructions. They are often left to be sent by emergency personnel who are busy trying to fight fires or control floods.” But when the system is used properly, “it acts like a siren in thousands of pockets, giving the authorities the ability to warn the right people at the right time.”

Ask yourself: Does my team have a checklist and/or templates in place to improve the effectiveness of emergency alerts without sacrificing precious time?

Coordinate Locally

Interagency cooperation and communication are the basis for effective alerting. A checklist can help your local counterparts supply the details for alerts. A standardized form for the uniform gathering of information should outline all of the details to create a given alert. This will prevent delays and confusion caused by going back and forth to obtain the necessary information.

Alerts Should Be Community-Driven

The onus is still on the local emergency manager to send out information and take ownership. Emergency managers might rely on the National Weather Service to do their job for messaging, for example, but this creates a disconnect. Why? Because they live in the community. Owning alerts helps enhance this local relationship and builds trust — which can help strengthen communities.

Have Message Templates Ready & Be Clear

When crafting alerts, remember they should be brief and instructive. It's important to create templates or pre-scripted messages in advance to streamline your alerting process. This alleviates some of the pressure during an already stressful situation.

When an emergency happens, you can fill in the blanks and make tweaks where needed, rather than starting from scratch under stress. Be sure to make any necessary adjustments to make the alert appropriate for your jurisdiction and the event at hand. The CodeRED IPAWS tool can help you build templates, and you can also monitor the national alerts feed to see how other agencies are constructing messages. FEMA also provides [templates](#).

We want to empower the community by providing actionable information, rather than cause fear. Fear doesn't generally lead to good decision-making.

Leverage Technology

WEA messages to cell phones can now include hyperlinks, so recipients can click for more detailed information, such as posters, photos and ongoing updates. The content can then be texted and posted on other platforms and community pages. This helps to engage and empower people during critical events while simultaneously preventing frustration caused by alerts containing only enough information to be frightening.

Double check to make sure the link is accurate before you send it!!!

The Warning Lexicon and Message Design Dashboard

Dr. Jeanette Sutton played a lead role in a research project that developed a Warning Lexicon to address the lack of training and education around alert creation among many emergency managers. The product of that research — [The Warning Lexicon: A Multiphased Study to Identify, Design, and Develop Content for Warning Messages](#) — is an extremely useful resource for overcoming the fear and hesitation of pressing the send button by helping emergency managers write effective warning messages quickly when a threat occurs.

The Warning Lexicon covers 48 hazards and includes information on the impacts of each hazard, as well as 112 protective action statements that can be used to write concise and clear alerts while reducing delays in the sending process.

Each hazard contains three content areas in the lexicon:

- 1 Hazard:** The specific name of the hazard posing a threat
- 2 Hazard impacts:** The consequences of the hazard on the population and infrastructure
- 3 Protective action guidance:** Recommended actions for message receivers.

When appropriate, certain words are written in all caps, so recipients can quickly see the most important information in the alert. The use of capital letters also expresses a stronger sense of urgency for protective action guidance requiring immediate attention.

Specific phrases are presented in brackets to let message creators know they need to make a selection (i.e., [do/do not]). Other copy that needs to be completed with the specific details of the event (location, time) are written in italics for easy identification.

The Warning Lexicon makes it easier to create alerts during stressful crisis events. The research also provides several best practices and tips to further speed up the creation of effective alerts:

- Create a list of the threats and hazards most likely to occur within your community in advance.
- Make a list of the trusted organizations and agencies you will include as the message source in your alerts.
- Establish a list of the most well-known locations where a threat or hazard may occur. The list should include popular landmarks, major roads and intersections, and the names of the towns, cities and counties in your jurisdiction.
- Set up a webpage or social media presence where you will post updates as a threat or hazard situation evolves.
- Practice writing alerts that fit within the character restraints through character counters in Excel or Google Sheets. Software applications like [Hemingwayapp](#) and [Grammarly](#) are also useful for this purpose.



The Warning Lexicon is the foundation for the [Message Design Dashboard](#) (MDD), which was developed by Dr. Sutton to provide templates to help emergency managers write effective messages for public alert and warning.

The MDD project outlines five key components of an effective and complete warning message:

- 1 Local, familiar, authoritative message source.
- 2 Description of the threat/event and consequences.
- 3 Location of the threat.
- 4 Protective action to be taken.
- 5 Message expiry time.

In practice, a message would use the following construction.

[Local, familiar, authoritative message source].

[Description of threat/event] in [location of threat] [consequences]. [Protective action].

Message expires [time].

The MDD guides users through the alert creation process with an interactive design that lets the user select whether to create a 90-character or 360-character WEA. From there, a series of screens walks the alert creator through the entire process through the use of drop-down menus and prompts to edit any text in brackets. A character count, review checklist and a final message preview that can be copied to the creator's clipboard make it easy to create alerts that include all of the essential details of an emergency so an alert can be sent with confidence.



Continuing Education

Additional Message Creation Tips

Public alerts, warnings and notifications should include:

- [Local, familiar, authoritative message source]:
[Description of threat or event] in [location and consequences]. [Protective action].

For example, a 90-character alert sent to cell phones would include only pressing details:

- NWS: FLASH FLOOD EMERGENCY this area til 11:00 a.m. EDT. Avoid flooded areas.

Be very specific regarding the location and protective actions involved in WEA alerts. Specifying a location takes the message one step further:

- NWS: FLASH FLOOD Lake Winona area til 11:00 a.m. EDT. Take appropriate actions. Avoid flooded areas.

An alert sent to devices capable of receiving messages up to 360 characters can contain more information:

- National Weather Service: A FLASH FLOOD EMERGENCY is in effect for the Lake Winona area until 11:00 a.m. EDT. This is an extremely dangerous and life-threatening situation. Do not attempt to travel unless you are fleeing an area subject to flooding or under an evacuation order.

The most effective alerts are simple and easy to understand, with actionable directives, location impacted and additional sources of information if possible. Basic templates like this ensure that everyone affected by the situation receives important information.

Press “Send”: Your Confidence Checklist

Use this checklist to ensure you’ve completed all of the necessary steps and can press “send” without asking for permission.

Emergency Alert Competence Building Checklist

PHASE 1 — Preparation	
Task	
<input type="checkbox"/>	Are you an authorized FEMA IPAWS Alerting Authority Organization? Sign Up to Use IPAWS to Send Public Alerts and Warnings FEMA.gov
<input type="checkbox"/>	Have you have taken FEMA’s Emergency Management Institute (EMI) independent study courses, IS-247 Integrated Public Alert and Warning System for Alert Originators and IS-251 Integrated Public Alert and Warning System for Alerting Administrators ?
<input type="checkbox"/>	Do you have written standard operating procedures (SOPs) for launching emergency alerts and warning messages that cover all of the following? <ul style="list-style-type: none">• Roles and responsibilities• Authority to launch• Applicable regulations and laws• Times of the day you can/should send messages• Identification of the notifications that need to be made• Backup method for sending messages• Password management and protection
<input type="checkbox"/>	Do you have printed copies of the SOPs and passwords at all designated launch sites?
<input type="checkbox"/>	Have you identified the roles and responsibilities on your team in regard to writing, approving and sending an emergency alert?
<input type="checkbox"/>	Have you conducted periodic training on the approved emergency alert and warning messages launch protocols and procedures with all designated and authorized individuals? (IPAWS Monthly Proficiency Demonstrations)
<input type="checkbox"/>	Have you participated in a training and exercise with the IPAWS Technical Support Services Facility?
<input type="checkbox"/>	Have you conducted hardware technical/functional training and tests to ensure reliability of equipment, software and user front-end interface?

PHASE 1 – Preparation (continued)

Task	
<input type="checkbox"/>	Have you drafted pre-scripted messages that cover the hazards listed in your Hazard Identification Risk Assessment (HIRA)? In different languages?
<input type="checkbox"/>	Are your pre-scripted messages in line with national best practices?
<input type="checkbox"/>	Have you conducted a no-notice drill during work hours and/or after work hours to test the system?
<input type="checkbox"/>	Have you built relationships with other adjacent Alerting Authorities and stakeholders?

PHASE 2 – Immediate Pre-Emergency Message Launch


Task	
<input type="checkbox"/>	Have you identified the information you need to share and have you followed the IPAWS Best Practices Guide for alert creation?
<input type="checkbox"/>	Have you identified the actions you want your recipients to take?
<input type="checkbox"/>	Have you set the appropriate activation area to target those individuals you want the alert to reach?
<input type="checkbox"/>	Have you selected the appropriate event code? fema_ipaw-november-2020-tip.pdf
<input type="checkbox"/>	Do you understand the difference between the WEA 360- and 90-character messages?
<input type="checkbox"/>	Have you decided if your message needs to cross jurisdictional boundaries and alerted adjacent communities if necessary?
<input type="checkbox"/>	Have you identified the appropriate individuals of the actions you're about to take and followed through with all necessary notifications?
<input type="checkbox"/>	If you are attaching a link (URL) to the message, have you tested the link before launching the emergency alert and prepopulated it with critical information pertinent to the situation?
<input type="checkbox"/>	Have you verified that the website you're referring people to for more information can support the potential traffic it may receive?
<input type="checkbox"/>	Do you know the phone number and email to the 24/7 FEMA IPAWS Technical Support Services desk should you have trouble launching your emergency alert? (1-844-729-7522; fema-ipaws-lab@fema.dhs.gov)
<input type="checkbox"/>	Have you identified your public information officer, and do they have the information they need to speak with the media and control the narrative?

PHASE 3 – Immediate Post-Emergency Message Launch

Task	
<input type="checkbox"/>	Have you validated that the correct emergency alert message has been sent?
<input type="checkbox"/>	Did it go to the intended audience?
<input type="checkbox"/>	Do you need to relaunch the emergency alert message with new geographic parameters and/or updated information?
<input type="checkbox"/>	Have you told the media when and where the next update will take place?
<input type="checkbox"/>	Have you identified who will participate in the update brief for the media?
<input type="checkbox"/>	Are you ready to send a closure message to those who received your first emergency alert message?

PHASE 4 – After-Action Scrub

Task	
<input type="checkbox"/>	Did the designated emergency officials take the appropriate actions?
<input type="checkbox"/>	Was an alert launched in a timely manner?
<input type="checkbox"/>	Was the alert missing critical information?
<input type="checkbox"/>	Did the intended population receive the message?
<input type="checkbox"/>	Have you identified what you can do differently next time to improve?
<input type="checkbox"/>	Has the SOP been updated by the individual responsible for maintaining it?
<input type="checkbox"/>	Has refresher training been scheduled and/or conducted?
<input type="checkbox"/>	Are you tracking the statistical information of the emergency alert message?



Conclusion: The Big Question

By Eddie Bertola, founder of Bertola Advisory Services

This probably isn't the first time you've seen best practices, read guides, reviewed checklists or attended training. It probably won't be the last time either. In fact, you may have been on this cycle for years.

You've had the opportunity to review this resource, which is filled with the latest expectations, tips and areas to focus on to increase the chance of success and to reduce the chance of failure.

You now know how common it is to feel reluctant or simply afraid to push the send button because of potential negative consequences from technical or human errors. You know some of the most common errors and ways to avoid them. Some of them may seem simple to avoid, but in an emergency situation, it's often the easy things that get overlooked and quickly become a problem. You also reviewed the mindset shift you may need to make to help you shape every success and mistake as an opportunity to learn and improve the process.

You were asked to look at the way you create messages. You were introduced to Dr. Jeanette Sutton and her groundbreaking research, including the five key components of effective messages. If you haven't already thought about the type and quality of alerts your organization sends, please set aside time to do so now.

You're encouraged to constantly improve with the training and continuing education resources provided here. The worst thing you can do is think you know everything in this field. There will always be room for training and education. Whether in a formal classroom setting or through the practical experience of an emergency, you must take advantage of every opportunity to get better. What separates the good from the great is often the ability to take advantage of the failures and mistakes and leverage positive change.

If you are anything like me, you realize how important this research is and if applied correctly, how much more effective we can be.

Which brings me to the big question.

It's simply this...What are your next steps?

If you read this information without deciding on what steps you can take to apply what you've learned, you're missing an important opportunity. Your next steps aren't predetermined, and they aren't a one-size-fits-all. They're unique to you and your situation.

The next steps you need to take may be different from others, but perfect for you. What may appear as a small step for some, may be a large leap for you. Strive to be the best you can be and keep the student mindset. As you work to incrementally increase your competence in the process and technology of emergency alerting, your personal confidence will increase, your stakeholder's confidence in your abilities will increase and, most importantly, you will be ready to answer the call to help save lives.

About the Authors



Eddie Bertola is the founder of Bertola Advisory Services and a subject matter expert in mass notification strategies, emergency messaging, missing person alerts and engagement with the public during emergencies. He consults with FEMA/IPAWS, federal, state, local, territorial and tribal leaders, and private sector companies. He is a Reserve Pea Ridge Arkansas Police Officer, a member of the Arkansas Troop L Child Abduction Response Team and the FBI Task Force for Child Exploitation and Human Trafficking. He worked for the California Highway Patrol for 15 years, concluding in the Counterterrorism and Threat Awareness Section as the lead statewide instructor for emergency messaging, the AMBER Alert and other missing person alerting.



Peter Gaynor is the Vice President, Resiliency and Disaster Recovery at Hill International. His experience includes serving as FEMA Administrator, the acting Secretary for Department of Homeland Security and Director for both state and local emergency management agencies. He oversaw FEMA's first ever operational response to a nationwide pandemic. He has more than 14 years of experience in emergency management and served for 26 years in the U.S. Marine Corps.

About OnSolve CodeRED

OnSolve® CodeRED is the leading provider of public alerting and residential safety technology that enables state and local government agencies to protect their community, responders and employees. CodeRED was designed by public safety officials and sends billions of alerts annually, helping agencies deliver emergency alerts quickly and reliably to save lives.

Trusted since 1998, more than 10,000 government agencies use CodeRED to provide real-time information to communities and keep them informed and safe. CodeRED is a trusted IPAWS provider and the alerting engine behind AMBER Alerts with the National Center for Missing and Exploited Children (NCMEC), helping aid in the alert, search and recovery process for more than 90,000 missing or abducted children and adult cases.

Learn more at onsolve.com/codered.

