IS-247.C
Course Summary

FEMA

IS-247.C Course Summary

Unit 1: Introduction to IPAWS

Objectives:

- Describe the Integrated Public Alert and Warning System (IPAWS), including intent, background, user roles and components
- Compare IPAWS to mass notification systems

Summary:

IPAWS Background

IPAWS Intent: Executive Order 13407 required an effective, reliable, integrated, flexible and comprehensive system to alert and warn the public.

What is IPAWS? FEMA's Integrated Public Alert & Warning System (IPAWS) is the national system for local alerting that provides emergency and life-saving information to the public. State and local public safety officials use IPAWS to send timely, geographically targeted emergency alert and warning messages to notify the public of natural and human-made disasters.

How does it work? After federal, state, local, tribal or territorial (FSLTT) Alerting Authorities write their own alert and warning message using commercially available software, the message is then delivered to the IPAWS Open Platform for Emergency Networks (IPAWS-OPEN), where it is authenticated and delivered simultaneously through multiple alert dissemination pathways. These pathways include:

- Emergency Alert System (EAS): Alerts to radio and television
- Wireless Emergency Alerts (WEA): Alerts to mobile phones
- National Oceanic and Atmospheric Administration (NOAA) Weather Radio: Alerts to weather radios
- Other public alert and warning systems and technologies

IPAWS is designed to allow one message to reach as many people in a targeted (defined geographic) area as possible regarding public safety incidents and emergencies. Using multiple communication pathways for public alerts increases the likelihood the message will successfully reach the public.

IPAWS Roles

IPAWS User Roles

Alerting Administrator	Alert Originator	Alerting Authority
An Alerting Administrator is **an individual who is responsible for implementation and use of IPAWS** in accordance with agency plans, policies, procedures and provides expertise with respect to public alert and warning practices.	An Alert Originator is **the individual person at the keyboard/screen** composing and issuing IPAWS alerts and emergency messages.	An Alerting Authority is **a public safety entity or jurisdiction** that uses IPAWS to alert and warn the public at the federal, state, local, tribal or territorial level.

FEMA and Federal Partners

Federal Partners: FEMA, the Federal Communications Commission (FCC), and NOAA's National Weather Service (NWS) work collaboratively to maintain the EAS, WEA, and NOAA Weather Radio, which are the three main components of the Integrated Public Alert and Warning System (IPAWS).

- Authorized federal, state, local, tribal and territorial authorities create alerts through IPAWS.
- The NWS issues weather-related alerts.

IPAWS and Mass Notification Systems

Both IPAWS and Mass Notification Systems disseminate life-saving alerts, but they have key differences and dependencies.

IPAWS uses broadcast technology to distribute different types of alerts via cell towers (WEA), radio and television (EAS), and the NOAA weather radio (NWEM). The public does not need to opt in to receive alerts through IPAWS.

A mass notification system is a subscription-based service that uses available communications systems to send voice messages, SMS, or web/app data communications only to members of the public who have signed up to receive the alerts.

IPAWS	Mass Notification Systems
• Non-subscription-based (no need to sign up) • Not subject to data and messaging fees • Not subject to network congestion • Sent through a separate communication pathway from everyday voice messages, SMS, or web and data app communications, with its own protocol • Used exclusively by authorized Alerting Authorities who have a signed and executed MOA with FEMA	• Subscription-based service, requiring users to sign up • Subject to data and messaging fees • Subject to network congestion • Sent through the same communication pathway using the same protocol as everyday voice messages, SMS, or web and data app communications • Capable of tracking the delivery of messages • Used by many groups beyond public safety officials such as school districts, colleges and universities, sports stadiums and private companies

Unit 2: Implementation

Objectives:

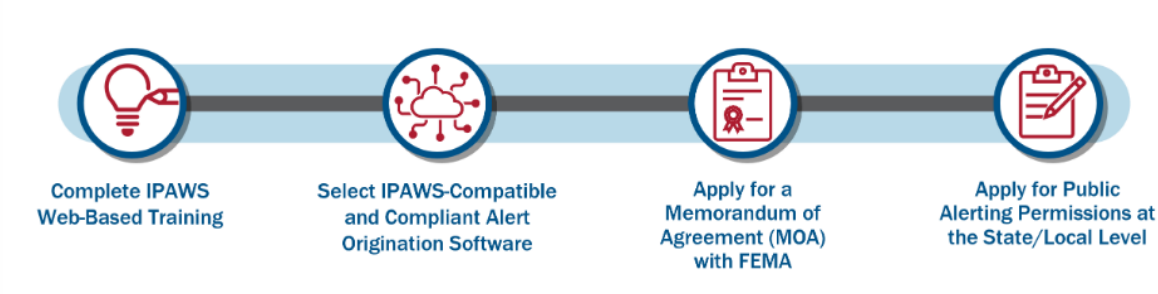
- Identify the benefits of IPAWS
- Explain initial considerations for implementing IPAWS, including becoming an Alerting Authority and developing stakeholder relationships

Summary:

Benefits of Implementing IPAWS

- Individuals do not need to sign up to receive alerts.
- IPAWS alerts can be delivered in both English and Spanish.
- Individuals do not incur any cost to receive alerts sent through IPAWS.
- Alerts sent through IPAWS can be targeted to specific geographic areas.

IPAWS Alerting Authority Application Process



Benefits of Stakeholder Relationships

- Broadcast, cable, and satellite operators are the stewards of the Emergency Alert System (EAS) in close partnership with state, local, tribal and territorial authorities.
- Private sector companies have agreements with FEMA to access, monitor and retrieve public alerts using the IPAWS All-Hazards Information Feed and maintain additional dissemination channels including sirens, social media, etc.
- Alerting Authorities (AAs) can establish arrangements and share permissions with other AAs at the state, local, tribal and territorial levels to alert on behalf of each other. This supports timely communications among and between communities in impacted areas and across all response forces.

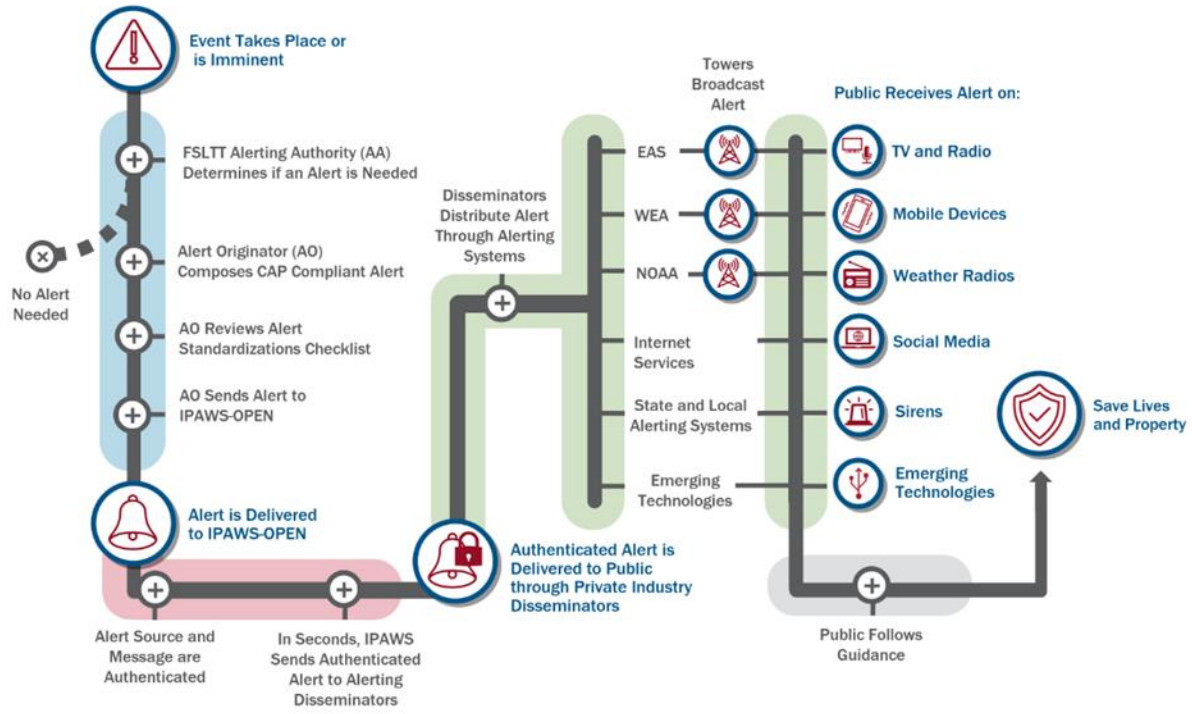
Unit 3: Technical & Operational Components

Objectives:

- Describe the purpose of Common Alerting Protocol (CAP)
- Identify the function of IPAWS Open Platform for Emergency Networks (IPAWS-OPEN)
- Recognize possible pathways of the IPAWS alert distribution process

Summary:

Alert Distribution Through IPAWS



How IPAWS Works: Alert Distribution Process

Common Alerting Protocol (CAP)	IPAWS-OPEN	Alert Disseminators
CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems including EAS, WEA and NOAA Weather Radio (NWR).	IPAWS-OPEN is the alert aggregator/gateway that receives CAP alert messages from various origination/authoring tools, validates the message, authenticates the senders and distributes the message to the dissemination pathways.	Alert Disseminators receive the CAP alert message from IPAWS-OPEN and send the message to the public across a variety of communication pathways.

How IPAWS Works: Alert Dissemination Pathways

Emergency Alert System (EAS)	Wireless Emergency Alert System (WEA)	NOAA Weather Radio (NWR)
Broadcasts alerts via cable, TV and radio.	Broadcasts alerts and warnings to cell phones and other mobile devices.	Broadcasts alerts and warnings via Non-Weather Emergency Messages (NWEM).
• Voluntary for EAS participants. • Cover a large geographic footprint. • Can support longer messages, audio attachments in mp3 format and additional languages. • Can interrupt radio and television to broadcast emergency alert information. • Cannot reach people who are not watching or listening to broadcast media. • May be repeated twice, but EAS "activation" interrupts programming only once; then regular programming continues.	• Participation by wireless service providers is voluntary, but most providers support WEAs. • Sent to all phones in the geo-targeted area. • Supports 90- and 360-character messages (90-character messages are mandatory). • Supports English and Spanish-language messages. • Supports clickable URLs. • Provides ongoing retransmission of WEA for the duration of the alert. • Able to update and/or cancel an active WEA. • Unique tone and vibration. • No need to opt in to receive WEA. • Not affected by network congestion and will not disrupt texts. • No tracking of individuals by phone number.	• An authorized Alerting Authority sends an NWEM to IPAWS-OPEN. • IPAWS authenticates the message and source, then posts the alert to the IPAWS Feed. • Your local Weather Field Office (WFO) receives a pop-up on their operational weather screens with the applicable IPAWS alert and ensures it is in the proper NWR format, then queues the NWEM for distribution by NOAA transmitters. • Weather radios tuned to those transmitters display alerts, which provide the public with critical, all-hazards information. • ***Note:*** *NWS only receives your alert if your agency is authorized by IPAWS, and you select "NWEM" (or similar) in your alert origination software. For authorization, update your IPAWS Public Alerting Authority application to include NWEM and obtain the signature of your designated approver.*

WEA Enhancement - Device-Based Geo-Fencing

Since December 2019, geo-targeting has become even more accurate for anybody with a WEA-capable device. Newer smartphones support device-based geo-fencing (DBGF), which uses GPS and Wi-Fi within the phone to determine whether a device is located within the specified target activation area. As long as the location services on the device are turned on, DBGF is designed to deliver alerts to 100 percent of WEA-capable devices inside the targeted activation area.

Note: *Not all handsets currently support DBGF. If the device cannot determine its location, then by default it will display the alert per earlier WEA protocols. Therefore, there may be occasions when older cell phones outside of a polygon will display a WEA intended for broadcast only within the polygon.*

How It Works

- The Alert Originator defines the boundaries of the target activation area using a polygon or circle in the alert origination software tool.
- Wireless providers send the WEA message with the specific boundaries of the target activation area, broadcasting it from cell sites within that area.
- Newer mobile phones and devices that receive a WEA then use their location functions to determine whether the device is inside or outside the boundaries of the target activation area.
- If inside or within 0.1 mile from the boundary, the device will display the alert.
- If >0.1 mile outside the boundary, the device will not display the alert, and will check periodically to see if it enters the activation area.
- If a mobile device enters the polygon and the alert is still active, the device will display the alert.

Additional pathways include:

Internet Based Services	Unique Alert Services (UAS)
Redistributes alerts via multiple technologies, including mobile applications, streaming services, smart home technologies and digital signage.	Delivers alerts to various pathways, including digital signs, subscription-based notifications, emails, reverse 911 systems, websites or programs based on geographic location and/or type of alert.
• All messages posted to IPAWS are posted to the All-Hazards Information Feed. • Authorized internet-based services can pull public safety messages from the All-Hazards Information Feed and redistribute the information.	• UAS are systems that have permission to retrieve alerts directly from IPAWS and deliver the alerts to their customer base through various pathways. • Unique systems can be upgraded to be CAP-compliant in order to seamlessly incorporate with IPAWS and make the alert and warning process streamlined and more resilient. • Use of the CAP standard enables industry partners to develop content and/or devices that can be used to provide emergency alerts to individuals with disabilities and others with access and functional needs.

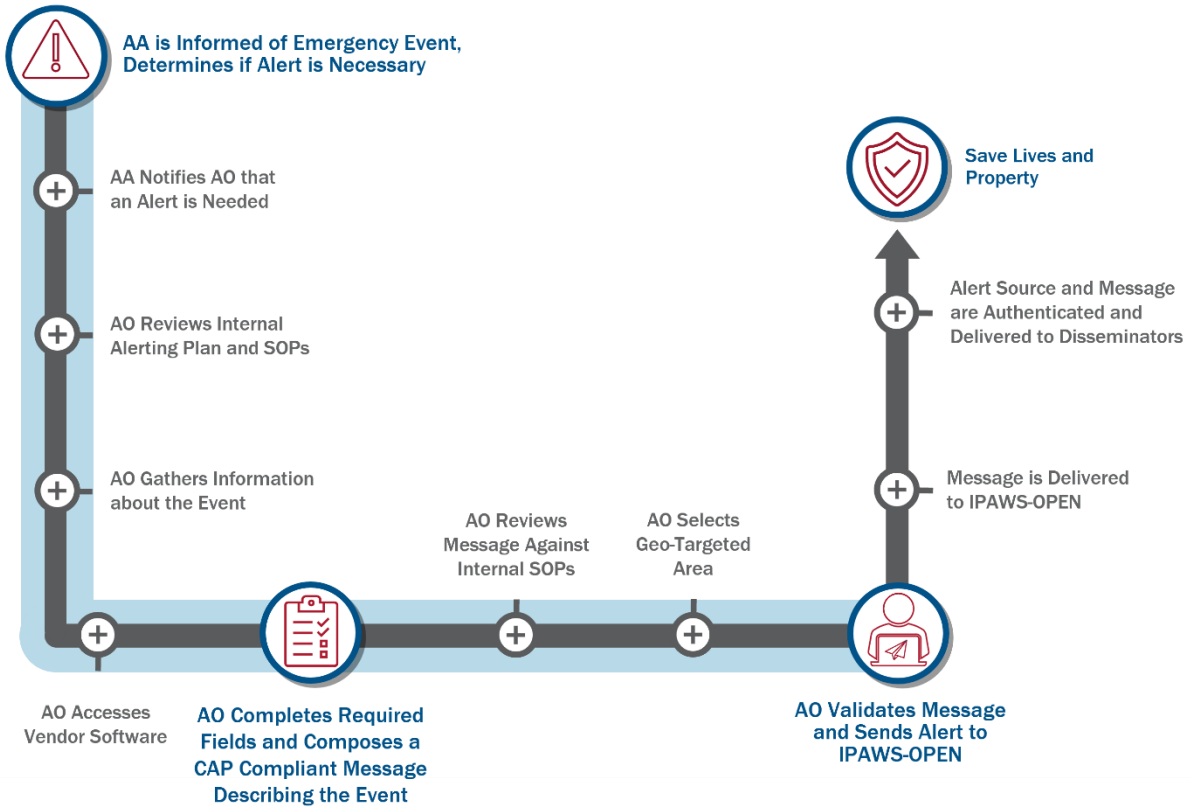
Unit 4: Message Development & Dissemination

Objectives:

- Identify the actions that initiate the IPAWS alert or message process
- Describe the basic requirements for creating alert and warning messages
- Describe the characteristics of an effective and actionable message
- Compare alerting methods available via IPAWS

Summary:

The diagram below outlines the steps for drafting and sending an alert using IPAWS. While the sequence may vary according to each AA's Standard Operating Procedures, the diagram highlights key steps to consider. In this Unit we will review steps of the process in greater detail.



When to Send

Deciding whether to issue a public warning can be a difficult decision. it is helpful to have a list of decision criteria to assist you with the process. For example, does the situation require that the public be told immediately to seek shelter or take other protective action? It will depend on the Standard Operating Procedures (SOPs) each Alerting Authority has established, along with clear judgment from local decision-makers. Please review your internal SOPs, public alerting permissions, and any other emergency plans that provide criteria for issuing public alerts to determine when to activate an IPAWS alert.

Where to Send

- **Review permissions.**
    - Alerts must be created based on designated permissions. FSLTT authorities who send alerts to the public through IPAWS must only send alerts for which they have permissions.
    - They must use the appropriate dissemination pathway, stay within the geographic warning area in their jurisdiction, and use the event codes for which the Alerting Authority has been approved.
- **Access IPAWS through third-party software.**
    - Depending on the software your Alerting Authority uses to send an IPAWS message, the login process may vary, for example:
        - Single sign-on
        - Username and password
        - Dual factor verification
        - Physical access (i.e., a specific workstation)
        - Mobile application
    - Once logged in, alert origination software is designed to enable users to take the actions that follow as they prepare to send an IPAWS alert.
- **Select dissemination pathways.**
    - Designate a geographic area to activate the alert.
    - Select an event code to define the nature of an event.
    - Input critical data elements (such as severity, certainty and urgency).
- **Consider the hierarchy of alerting.**
    - Establish criteria for usage of each alert dissemination option and develop an associated standard operating procedure (if not already in place).
    - It is a good idea to design a hierarchy of alerting based on your: Identified hazards, severity of threat, and frequency of occurrence
    - As you develop your hierarchy of alerting, it is important to keep in mind the following:
        - You can add or remove alerting methods as needed.
        - Use all forms of alert and warning systems available to your organization as appropriate.
        - Increasing modes of communication allows you to reach more diverse groups.
        - Refer to your alerting hierarchy to identify which types of platforms to use.
        - Ensure all messages are consistent across all platforms.
        - Recognize that no single platform reaches 100% of the population.
- **Select a dissemination pathway (e.g., EAS, WEA, NOAA Weather Radio, and/or auxiliary systems).**
    - Use the alert and warning systems available to your organization as appropriate.
    - Make sure all messages are consistent across all platforms.
    - Recognize that no single platform reaches 100% of the population.
- **Designate a geographic area to activate the alert.**
    - Input the Federal Information Processing Standard (FIPS) code(s) which uniquely identify states, counties and county equivalents.
    - For WEAs, you may have the option to precisely define the boundaries of the target activation area by drawing or uploading polygons or circles.

- EAS and NOAA Weather Radio do not use polygons or circles.

What to Send

- **Select an event code to describe the type of incident.**
  - Alert Originators should understand their event code permissions and select an event code based on internal procedures and processes.
  - Your selection of an event code may depend on what members of your community will understand based on local practice or how new information will be received.
  - State/local/tribal emergency plans may limit the types of codes that EAS participants, broadcasters for example, are assigned to monitor for EAS broadcasts.
  - Hazardous weather event codes are reserved for the National Weather Service (NWS).
- **Input data elements (such as severity, certainty and urgency).**
  - For severity, only events meeting the criteria of extreme (i.e., an extraordinary threat to life or property) or severe (i.e., a significant threat to life or property). Levels of severity:
    - *Extreme*: Extraordinary threat to life or property
    - *Severe*: Significant threat to life or property
    - *Moderate*: Possible threat to life or property
    - *Minor*: Minimal to no known threat to life or property
    - *Unknown*: Severity is unknown
  - For certainty, only events meeting the criteria of observed (i.e., determined to have occurred or to be ongoing) or likely (i.e., has a probability of greater than 50 percent). Levels of certainty:
    - *Observed*: Determined to have occurred or to be ongoing
    - *Likely*: Meaning probability is greater than or equal to 50%
    - *Possible*: Probability is less than 50%
    - *Unlikely*: Not expected to occur
    - *Unknown*: Certainty is unknown
  - For urgency, only events meeting the criteria of immediate (i.e., responsive action should be taken immediately) or expected (i.e., responsive action should be taken soon, within the next hour). Levels of urgency:
    - *Immediate*: Responsive action should be taken immediately
    - *Expected*: Responsive action should be taken soon (within next hour)
    - *Future*: Responsive action should be taken in the near future
    - *Past*: Responsive action is no longer required
    - *Unknown*: Urgency is not known
- **Compose your warning message.**
  - **Source** — State who the message is from. Use local, familiar, trusted sources. Spell the source name out completely (no acronyms).
  - **Hazard** — Be sure to describe the hazard/threat type and impact. This information helps the public determine their individual next steps as they analyze the potential risks for where they are physically located at the time they receive the alert/warning.
  - **Location** — Use familiar landmarks and known physical boundaries in addition to city/county names. In some cases, location includes where people should go as well as the areas affected.
  - **Guidance** — Tell people what protective action to take, when they should take this action, how to accomplish the action, and how the action will reduce impact(s).
  - **Time** — If you do not include an expiration time, tell people where to find more information about the hazard and how they will learn that conditions are safe.

- **Consider warning message style.**
    - **Clarity** — Use clear language and avoid unnecessary abbreviations.
    - **Certainty** — Use authoritative language about the threat. Relay as much certainty about the threat, impact and protective actions.
    - **Specific** — Be specific and include details about the hazard, location at risk, impact and actions people should take to be safe.
    - **Consistency** — Ensure messaging internally and externally is consistent.
    - **Accuracy** — Do not overstate or understate the facts. Do not omit important information. Use selective capitalization.
- **Use the Message Design Dashboard.**
    - The Message Design Dashboard (MDD) was built by the University at Albany in partnership with FEMA IPAWS to make writing complete and effective messages easier.
    - Alert Originators should use the MDD to build their message templates before emergencies occur. You can access the Message Design Dashboard within the Alerting Authority ATP (Assistive Tool Platform).

Guidance Documents

- IPAWS Best Practices Guide
- IPAWS Process Map Playbook Purpose

Unit 5: Best Practices

Objectives:

- Describe the processes for message maintenance including monitoring, updating, cancelling and logging
- Identify factors that may prevent messages from reaching the public effectively
- Examine factors that may influence public response to alert and warning messages

Summary:

Message Maintenance

Monitoring Alerts: Once a message is sent, your job isn't over! Monitoring the status of a message not only enables you to confirm that the alert was disseminated and the public received it. It also confirms use of the proper pathway. Alert Originators must:

- Confirm the message was sent successfully.
- Continue to monitor the situation.
- Determine if the original message is still valid.
- Send updates, if needed.
- Cancel the message if the situation warrants termination.

Updating Alerts: Disasters and emergencies often change; therefore, you might need to update an alert.

- Reference pertinent information from the original alert, highlight new or additional information and specify recommended actions.
- Only send an update if there is significant new information or changes in the situation to avoid alert fatigue.
- Send a follow-up message when the situation is over as a best practice.

Cancelling Alerts: Once you send a message you should continuously monitor the situation and send updated messaging as appropriate, keeping in mind the information that was already sent. If a message is sent in error, you should follow your Alerting Authority's policy on cancelling a message and sending an "all clear" update. Additional considerations include:

- The cancel button in your alert software will not send a cancel alert to your affected population. It is a technical tool that will stop the last message from continuing to be distributed.
  Note: *For WEA, use the update button to cancel the original alert and issue a new alert.*
- If you are simply cancelling a message, then updates may not be required, though it is recommended practice to do so.

Reaching the Public

Common Mistakes – Mistakes Regarding Message Creation and Effectiveness

- Critical alerts not communicated in a critical way
- Not leveraging templates
- Neglecting a message check
- Ineffective message creation

Examples of Effective Alerts

Example Message	Best Practices
Sunbelt Gov: FLOODING on Route 2 exit 1. Road blocked. Use I-85. Updates www.sunbelt.gov	• Source: Indicates the alert is from Sunbelt Gov, providing credibility. • Precise Location: Mentions "Route 2 exit 1" as the affected roadway. • Clear Impact: Conveys that the road is blocked due to flooding. • Protective Action Guidance: Instructs the public to "Use I-85" as an alternative route. • URL for More Info: Provides a website for updates and additional information.
Gulfport County Police. WINTER STORM WARNING for Gulfport from 5 PM Saturday to Sunday at 4 PM. Snow and winds will be heavy and may cause power outages as well as limited visibility. Travel could be very difficult. Stay off roadways and stay safe. EMERGENCY SHELTER available at Gulfport High School (123 Beach Blvd). For more info: www.gulfport.gov	• Source: Indicates the alert is from Gulfport County Police. • Precise Location: Specifies the affected area of Gulfport. • Protective Action Guidance: Instructs residents to expect power outages and to not travel. • Clear Urgency: Clearly identifies the timing and urgency of the event: “5 PM Saturday to Sunday at 4 PM." • Contact Information: Includes shelter address, and website for additional information.

Factors Influencing Public Response

- **Public Knowledge of Emergency Messaging**: Ongoing public education about alerts and warnings helps communities understand the purpose and importance of alerts while minimizing confusion. For the technology and alert message to be effective, the public needs to know what to expect when they receive alerts and what actions they might need to take.
- **Social Factors**: Several social factors influence how people receive, comprehend and heed alerts and warnings. These factors include:
  - Level of community interaction
  - Observations
  - Family composition
  - Perception of risk
  - Length of residency
  - Personal dynamics
- **Personal Dynamics**: Specific personal dynamics that have an influence on how individuals receive, understand and heed alerts and warnings include:
  - Individual preparedness – People who have taken the time to prepare for hazards are more likely to heed warnings and act appropriately.
  - Types of community – Residents of rural communities may have more difficulty receiving warnings than those living in urban areas.

  - Age – The very young and the elderly may not be able to receive and/or respond appropriately to alerts and warnings. Many in this group may also need assistance.
  - Language – Non-English-speaking persons may not understand warnings that are provided in English. Communities with high percentages of non-English-speaking people should issue warnings in the primary language(s) of the population as well as in English.
    - IPAWS does not provide translation services, but it can accept and relay alerts in multiple languages.
    - Your jurisdiction's alerting software may provide automated translation, but you should validate any automatically translated text with a speaker of the language to avoid errors.

- **People with Disabilities or Access and Functional Needs (AFN)**: Alternative alert and warning methods are needed for people with disabilities and/or access and functional needs (AFN). This includes the blind or low-vision and deaf or hard of hearing. AFN populations may require alerts in varying formats. With this in mind, both audio and equivalent text messages should be made available. Some accessibility elements include:

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

Unit 6: Training, Practice & Exercising for Alert Originators

Objectives:

- Describe the purpose of the IPAWS Test/Demo Environment
- Describe the process for obtaining an IPAWS Training/Demonstration digital certificate
- Identify the various methods to train and practice using the IPAWS Test/Demo Environment

Summary:

IPAWS TSSF Support

The IPAWS Technical Support Services Facility (TSSF, formerly known as the IPAWS Lab) hosts the IPAWS Test/Demo environment for alert creation and dissemination to all IPAWS pathways so that Alerting Authorities may train, practice and exercise alert, warning and notification procedures and processes.

Additionally, the TSSF includes state-of-the-art interactive conference and seminar spaces to support Alerting Authorities on site and virtually with seminars, training initiatives and exercises. The TSSF enables participants to develop proficiency in sending alerts in a safe environment and thereby build confidence for sending effective alerts in the live environment.

Some examples of beneficial use cases include:

- Train new and experienced AOs alike
- Experiment with new technologies
- Understand the technical elements of IPAWS
- Practice alerting techniques in a test environment

IPAWS Test/Demo Environment

- Within your IPAWS-compatible alert origination software you'll find both an IPAWS live environment and the IPAWS Test/Demo environment.
- The IPAWS Test/Demo environment is a sandbox version of IPAWS that mimics live environment capabilities and is used to train, practice and exercise. It is a valuable resource to Alerting Authorities, allowing them the space to develop and enhance their skills with public alerting tools.

IPAWS Training/Demonstration Digital Certificate Process

To gain access to the IPAWS Test/Demo environment, Alerting Authorities must first complete the following requirements:

- Complete the IPAWS application process to gain access to both the IPAWS Live and Test/Demo environments.
- Obtain IPAWS Live Digital Certificate and the Training/Demonstration Digital Certificate.
- Upload the Training/Demonstration Digital Certificate to the alert origination software.
- Confirm connectivity to the IPAWS Test/Demo environment.

Using the IPAWS Test/Demo Environment

Once you have access to the IPAWS Test/Demo environment, ways to test include:

- In person (IPAWS TSSF on-site training)

- Virtual (webinar with IPAWS TSSF personnel)
- Independent (Alerting Authority led testing)
  Note: *Leverage the IPAWS Message Viewer web interface to confirm successful alert message dissemination to the IPAWS Test/Demo environment.*

Requirements - Monthly Proficiency Demonstration

Alerting Authorities are required to send a successful demo message at least once a month to the IPAWS Test/Demo environment. This Monthly Proficiency Demonstration (MPD) requirement has been in place since October 1, 2019. The purpose is to increase Alert Originators' skills and confidence when issuing alerts, and to lessen the risk of errant messages.

The IPAWS Customer Support Branch monitors the IPAWS Test/Demo environment activity for MPD compliance. The following rules apply:

- Miss 1 month = Friendly reminder
- Miss 2 months = Notification to your state IPAWS authority
- Miss 3 months = Risk of having IPAWS connectivity disabled

Note: *Live messages sent to the production environment* ***do not*** *count toward MPD compliance.*

Integrating IPAWS

Integrating IPAWS into your plans, drills, workshops and exercises supports an effective and well-coordinated response during emergencies.

The IPAWS Project Management Office fully supports inclusion of IPAWS in exercises and offers the following resources:

1. The **IPAWS Exercise Starter Kit (ESK)** provides public safety officials with ready-to-use materials and templates to develop, conduct and evaluate exercises tailored to their specific threats, resources, operational plans and procedures. The IPAWS ESK can be found on the Preparedness Toolkit.
2. The **IPAWS Program Planning Toolkit** is a set of resource documents, guides and an online alert plan creator to assist local Alerting Authorities with producing a comprehensive all-hazards alerting plan inclusive of staff planning, standard operating procedures, tests and exercises.
3. The **IPAWS Technical Support** team is staffed with skilled exercise facilitators certified through the Homeland Security Emergency Evaluation Program (HSEEP). This means that you have experienced exercise professionals available to you to help plan exercise objectives and scenarios.
4. The **IPAWS Best Practices Guide** provides guidance to IPAWS Alerting Authorities on the effective use of EAS, WEA and NWEM messages via IPAWS and on how to issue timely and effective messages in response to threats to public safety.