



IPAWS

Train the Trainer Guide

Integrated Public Alert and Warning System (IPAWS)

September 2020



FEMA

This page intentionally left blank (*FEMA Blank Page Note* style)

Table of Contents

Introduction	3
1. Importance of AWN Training Program & Relationship to IPAWS.....	3
Basic Elements of AWN Training Program	4
AWN System Information	5
1. All alerting systems your organization is authorized to use.	5
2. Alerting vendor information.	6
3. Guidance for alerting platform access.....	6
Alerting System Standard Operating Procedures	7
1. Approval chain of command for authorizing an alert.....	8
2. Credential management guidelines, including:	8
3. Vendor software alerting instructions.....	8
4. File storage guidelines and management	8
5. Agency’s plan for message translations.....	9
6. Event codes your agency is authorized to use, including:.....	9
7. Organization’s risk mitigation strategy.....	9
8. Training Schedule, including:.....	9
9. Testing, including:.....	9
10. Include an audit schedule.	9
Messaging Templates	10
1. 90-character Message Template	10
2. 360-Character Message Template.....	10
System Training Environments	12
1. Alert Originator; the ability to log in and;.....	12
2. Alerting Administrator; the ability to;.....	12
Exercises	14

Appendix A: Supplemental Training Resources 16

Introduction

The Federal Emergency Management Agency’s Integrated Public Alert and Warning System (IPAWS) office’s Train the Trainer Program Guide provides state, local, tribal and territorial (SLTT) Alerting Administrators with recommendations and best practices that can be used when developing an internal training program for Alerts, Warnings, and Notifications (AWN). The Guide focuses on components of a successful Train the Trainer Program, including AWN System Information, Alerting System Standard Operating Procedures, Testing and Exercise Guidelines, and Training Guidelines.

The Guide is not intended to be a solution for all public safety officials, but to supplement existing training efforts. It can provide additional considerations in creating or modifying a robust IPAWS training program for those responsible for implementing and using the system.

<http://www.fema.gov/ipaws> ipaws@fema.dhs.gov

1. Importance of AWN Training Program & Relationship to IPAWS

Developing and implementing an effective Alert, Warnings, and Notifications training program is a crucial part of sending critical emergency alerts. As of May 2020, more than 1,500 Alerting Authorities at the SLTT level can use IPAWS to send local alerts to televisions, radios and cell phones in their targeted areas. ¹ IPAWS has delivered more than 50,000 alerts via Wireless Emergency Alerts and the Emergency Alert System since launching in 2012. ² IPAWS provides the following benefits for Alerting Authorities:

- Richer, more accessible content;
- Relevant alerting through specific hazard area geographic information; and
- Up-to-date technology.

To fully support comprehensive IPAWS programs, FEMA and the Department of Homeland Security Science & Technology Directorate collaborated with SLTT stakeholders to create robust and consistent training guidelines and processes. This Train the Trainer Guidance will assist with creating cohesive alerting standards nationwide.

¹ Federal Emergency Management Agency. “Alerting Authorities.” FEMA, 2020, <https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public-safety-officials/alerting-authorities>. Accessed 13 August 2020.

² Federal Emergency Management Agency. “Alerting Authorities.” FEMA, 2020, <https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public-safety-officials/alerting-authorities>. Accessed 13 August 2020.

Basic Elements of AWN Training Program

Every incident is different, with varying factors and decision points that change in a matter of seconds. It is therefore critical to not only train staff on how an alert is transmitted, but the effects of the alert on the public, to encourage high-impact alerting.³ FEMA IPAWS recommends that jurisdictions create a training program consisting of readily available coursework divided into sections of system access and responsibilities. Based on statewide guidance and more than 100 stakeholder interviews over the past several years, it is recommended the following sections be included in a training program to increase effective usage of IPAWS and emergency alerting:

- AWN system information;
- AWN system SOPs;
- Messaging templates;
- Training and system tests; and
- Exercises.

³ Department of Homeland Security Science and Technology Directorate. "Report on Alerting Tactics." DHS S&T, 2018, https://www.dhs.gov/sites/default/files/publications/1051_IAS_Report-on-Alerting-Tactics_180807-508.pdf. Accessed 13 August 2020.

AWN System Information

The complex nature of Alerts, Warnings and Notifications programs can often make it difficult to clearly explain to Alert Originators the mechanisms available and how to access each system. Having a clear breakdown of the differences between the communication pathways and key contact information can be critical to sending effective and timely life-saving alerts during an incident or disaster. It is encouraged that this information be available during onboarding and refresher training in chart form for easy reference. See Figure One for an example AWN System Chart.

Table 1: Example AWN System Chart

	Communication Pathway 1 (Ex: WEA)	Communication Pathway 2 (Ex: EAS)	Communication Pathway 3 (Ex: Sirens)	Communication Pathway 4 (Ex: Landline Alerts)
Audience	Ex: Residents with cell phones in x region			
Benefits	Ex: wide reach of population, will reach citizens passing through the area			
Vendor Information	Point of Contact (POC) Name POC Email POC Phone # Vendor availability (ex: 7am to 7pm)			

The following are elements that Alerting Administrators should consider in their reference documents:

1. All alerting systems your organization is authorized to use.

- Definitions of all mass notification systems, including IPAWS.
- Intended audience for each system.
- Key benefits of each system.

2. Alerting vendor information.

- Primary point of contact (email and phone number).
- Email, phone number, and hours available for the vendor help/support desk function.

3. Guidance for alerting platform access.

- Outline step-by-step instructions for logging into the alerting platform.

Alerting System Standard Operating Procedures

Standard Operating Procedures have been found to be a key factor in successfully sending alerts to the public in a consistent and timely manner. Including SOPs in the training process can ensure new and existing employees have a clear understanding of what is expected of them and that they are able to quickly and efficiently access critical information during an emergency event. This ensures that the alerting process occurs as quickly and accurately as possible while also avoiding public confusion, delayed public response, and degraded trust in alerting systems due to alert errors. Figure Two is an example of how to organize a training schedule for different alerting positions.



Example Training Schedule

Training Requirements

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

Alert Originator (AO) – is a level designed for those who can physically access and send on platforms within the jurisdiction’s alert and warning program.

- Monthly tests to themselves if they have not sent a real-world message during the week.
- Training from the system vendors designed to teach technical skillsets within the system specific to message sending.

If person is to be a sender for any portion of the IPAWS system, he or she must also have the following (as per FEMA requirements):

- IS-247: IPAWS for Alert Originators (required under FEMA MOU)
- IS-251: IPAWS for Alerting Administrators
- IPAWS Rules of Behavior: Read, understand, and sign the IPAWS Rules of Behavior.

Alerting Administrator (AA) – is a level designed for those overseeing the entire alert and warning program.

Complete all courses under the previous A.O. levels as well as:

- Training from local GIS professionals within the jurisdiction, if the system(s) in use require geo-coding and/or loading shape files. Person should be knowledgeable in cross-jurisdictional coordination techniques within the jurisdiction.
- IS-29 Public Information Officer Awareness

- G-290 Basic Public Information Officer Course

Read articles that explain the social science of alert and warning, such as:

- Best Practice Guide for Warning Originators (Office of the U.S. Attorney General)
- WEA Messages: Impact on Physiological, Emotional, Cognitive and Behavioral Responses (U.S. Department of Homeland Security)
- Best Practices in Wireless Emergency Alerts (U.S. Department of Homeland Security)
- PrepTalks Discussion Guide: Modernizing Public Warning Messages (Dr. Dennis Mileti)

Alerting Authorities should ensure that SOP's containing the following content are covered as part of their training programs:

1. Approval chain of command for authorizing an alert.

- Include any agreements with other Alerting Authorities and the chain of command for sending a multi-jurisdictional alert.
- Include all employees or staff authorized to send an alert if the primary Alert Originator is not available.
- Provide guidance on offering knowledge redundancy in case of an emergency.

2. Credential management guidelines, including:

- Log-in account information guidelines (individual or agency wide);
- Username and password storage guidelines;
- System log-in guidelines (i.e. must log in once a month to check system); and
- Password update guidelines (i.e. passwords must be changed every four months).

3. Vendor software alerting instructions.

4. File storage guidelines and management.

- Outline where templates and pre-scripted messages are stored.
- Outline where training documentation is stored.

5. Agency’s plan for message translations.

- Translation considerations: Some translated messages tend to use more characters than English versions. Ensure your translated messages are still within the 90- and 360- character limits.

6. Event codes your agency is authorized to use, including:

- Threshold for triggering an alert;
- Description of when WEA, EAS, and National Weather Emergency Management (NWEM) alerts are warranted in your jurisdiction versus an “opt-in”; and
- Inclusion of broadcaster agreements on which event types will air EAS.

7. Organization’s risk mitigation strategy.

- Outline your policy for unexpected situations, including approval chain of command in an emergency, back up data, etc.

8. Training Schedule, including:

- Current training schedule and how often current employees are retrained on alerting practices;
- Roles and the required training associated with them (i.e. executive level training, alert senders, etc.); and
- Clearly defined parameters for when WEA, EAS, and NWEM alerts are warranted. Be as specific as possible.

9. Testing, including:

- Frequency that tests must be conducted and by whom;
- FEMA IPAWS Lab required monthly testing; and
- Message cancellation strategy, inclusive of a National Defense Authorization Act (NDAA) requirement to mitigate any negative impacts of false missile alerts.

10. Include an audit schedule.

- Stakeholders recommend auditing your SOPs at least once a year.

Messaging Templates

Understanding what information an alert should contain is important for public recipients taking protective action and should be a main focus of AWN training. Alerting Administrators are highly encouraged to make the alert templates as they appear in the alerting system and have sample messages available during the training process. These templates should also include multiple situations in which an alert needs to be sent to ensure that proper context can be applied around each situation (e.g. street closures during a planned event). Figures Three and Four are example messages can be used to effectively convey the key elements of a template and what they would look like if sent:

1. 90-character Message Template

[Insert name of source]: [Insert event type] in [this area] until [insert time here] [Guidance- what to do] [insert URL if possible]

Table 2: Example 90-character Messaging Templates (State of Minnesota)

Field	Example
[Source] Sender Name value, typically associated with the Alert Originator	Aitkin County Sheriff
[Guidance – What to do] Assigned value derived from instruction-specific event code (EVI, SPW) or response type element	Take Shelter Now
[Hazard – What] Event name corresponding to event code element	Chlorine Gas in air
[Location – Where]	In this area until
Termination in local time zone derived from expired element	4:30pm
<p>A WEA Message would look like this: [# of characters]</p> <p>Chlorine Gas in air this area until 4:30PM Take Shelter Now - Aitkin County Sheriff [85] Aitkin County Sheriff Advises Take Shelter Now - Chlorine Gas in this area until 4:30PM [89]</p>	

2. 360-Character Message Template

[Insert title and organization of a local, familiar, authoritative message source]. A [insert a brief description of the event] occurred at [insert the time the event occurred] at [insert name]. The [insert the same brief description of the event]. People in [insert a brief description of the boundaries of the area at risk] who are [insert direction or markers of incident] should check and monitor local media now and continue to do so frequently. There is no reason to do anything more at this time. This message will be updated when new information becomes available. [insert addition of URL, phone number, or social media link].



Example 360-character Message (PrepTalks: Dr. Dennis Milet)

Example Message [355 characters for WEA 360 message length]

Elm County Sheriff. Floodwaters are approaching Wood City and will hit two blocks on both sides of Elm Creek from Hwy 110 to Maple Road. People outside will be washed downstream. The water will be above rooftops. Move two blocks plus from the creek now and be there no later than 6:00 pm to avoid the flood. This message expires at 11:00 pm, May 15, 2017.

System Training Environments

Using tools routinely through system training environments allows Alert Originators to practice alerting procedures and gain familiarity with alerting technologies to minimize errors during an incident. Alerting Administrators are highly encouraged to include hands-on-use of their alert platform training environment (if available) as part of their training program. The following are areas that Alert Originators and Alerting Administrators should consider covering as part of their hands-on-use training:

1. Alert Originator; the ability to log in and;

- How to identify the digital certificate expiration date;
- How to verify user connectivity to IPAWS;
- How to send a Required Weekly Test (RWT) to ensure it is connected to the correct location;
- How to identify the differences between automated, template and ad-hoc alerts;
- How to send an alert via IPAWS;
- How to send an alert through the vendor system;
- How to cancel an alert; and
- How to create a new message using the following criteria;
 - Choose proper event code;
 - Create a polygon or circle, of less than 100 nodes;
 - Create free-form 90- and 360-character WEA text, while avoiding prohibited characters;
 - Send one alert to multiple channels (WEA, EAS, NWEM, etc.);
 - Select a pre-populated template and fill it in to the greatest extent possible; and
 - Update or cancel an alert, without having to reenter all of the data.

2. Alerting Administrator; the ability to;

- Check an alert message template for errors, prior to sending;
- Review alert history and/or logs for possible errors;

- Define IPAWS alert status codes for sent alert, with a determination of what the advice codes mean;
- Engage vendor support, to include user training, and around the clock technical support; and
- Create user ID and passwords based on the provided guidelines.

Organizations with IPAWS integration are required by FEMA to perform monthly tests of their system through the IPAWS Lab. However, stakeholders recommend including training with the IPAWS Lab for all Alert Originators and staff that could be involved during an emergency on a more frequent basis. Research shows testing in controlled and closed environments helps maintain proficiency with alerting tools and exercise plans and procedures (i.e. IPAWS Lab, vendor-controlled tests, etc.). Organizations should consider including the following IPAWS Lab topics in their training:

- What the IPAWS Lab allows and does not allow (i.e. how it's a protected space to test, etc.);
- How to access the IPAWS Lab;
- Using IPAWS Lab assistance for IPAWS required monthly proficiency tests; and
- Incorporating IPAWS Lab in tests, exercises, and training initiatives.

Exercises

Including alert training in an organization's test, training and exercise (TT&E) programs can provide an additional level of context that otherwise could be limited in traditional training settings. Where possible, Alerting Administrators are encouraged to leverage TT&E programs as a means to offer additional training for Alert Originators as well as broader audiences that might be directly or indirectly involved in the alerting process. These TT&E programs could include the integration of IPAWS capabilities into existing interagency, multi-agency, or community exercises. Alerting Administrators are encouraged to include the following as part of exercises:

- Exercises that are Homeland Security Exercise and Evaluation Program (HSEEP) compliant. (Use the [National Exercise Program](#) to request FEMA exercise support.)
- Scenarios involving alerting topics and/or practices such as sending a test alert;
- Discussions on Federal Communications Commission (FCC) requirements and waivers that could be required should the agency want to send a test alert to the public;
- Use of the IPAWS Lab for a safe, pre-testing environment;
- Discussions on test ranges such as the strategic deployment of phones in one-tenth of a mile increments, per FCC rules, to understand alert propagation;
- Discussions on public relations campaign for pre- and post-test information to include media day and a press kit for reporters;
- Exercise injects that focus on different parts of the alerting process such as chain of command decisions;
- After-action sessions that include alerting topics;
- Development of after-action reports and improvement plans that include alerting topics; and
- Shared alerting outcomes from after-action reports with appropriate alerting partners.

Figure Five shows best practices that the State of Minnesota has incorporated as part of its testing and exercise programs:



Example Public Alerting Best Practices (State of Minnesota)

Testing

It is important to test your templates. Testing methods may be devised locally with assistance from software vendors during training, or with instructions from the IPAWS Lab. FEMA

maintains the IPAWS functional laboratory and provides interoperability and functional testing support, Information Assurance support, and overall technical support.

Interagency Testing

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

Coordination

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

Consistency

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

Appendix A:

Supplemental Training Resources

FEMA has developed additional training resources that Alerting Administrators are encouraged to take advantage of as part of their alerting programs. These include

- [IS-251: Integrated Public Alert and Warning System \(IPAWS\) for Alerting Administrators](#);
- [IS-247: Integrated Public Alert and Warning System \(IPAWS\) for Alert Originators](#);
- [IS-120.C: An Introduction to Exercises](#); and
- [Homeland Security Exercise and Evaluation Program \(HSEEP\)](#).