

TEXAS DIVISION OF EMERGENCY MANAGEMENT

Texas IPAWS Overview



Texas Alerting Authority

- Texas Division of Emergency Management (TDEM) is the approver of Public Alerting Authority (PAA) Applications, for entities that request Alerting Authorization in Texas, to include Texarkana (TX/AR).
- In Texas, there are approximately 250 entities in the FEMA IPAWS database. They are in various statuses, as not all are “Online” with no issues. Because an entity is not in “Online”, it does not mean they cannot send alerts. An example is when they are renewing their MOA. An expired MOA will not automatically cause the loss of Alerting privileges.
- IPAWS is a tool to notify the public, but it does not replace Press Briefings. Coordinate Public Service Announcements with your PIO to prevent sending conflicting messages.



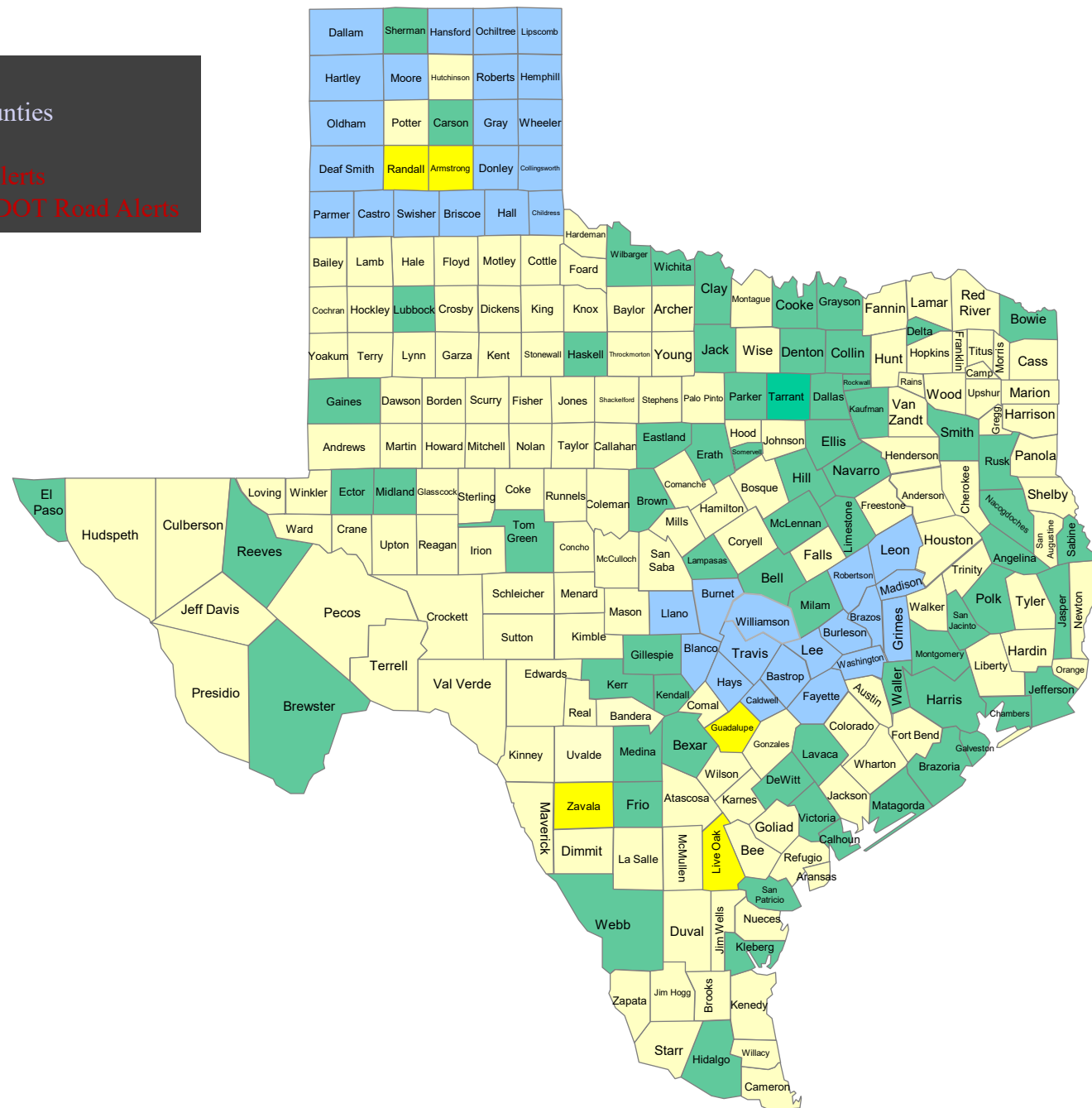
Texas IPAWS Stats

Status	QTY
Online No Issues	100
Expired MOA - Online / Active	47
Total in Que: EMI/PAA/Ready	14
MOA In Progress - Not Active	86
Offline - Expired - Deactivated	5
Total in FEMA IPAWS DB	252



Lite Blue = Active COG Counties

Yellow = MOA Issue



Cross Jurisdictional Support

- In an emergency, FEMA IPAWS can send alerts on behalf of an Authorized Alerting Entity / local jurisdiction. However, it is not immediate, as the alert and the requesting entity must be verified.

Local > County > COG – Regional Plan > State > FEMA

- FEMA should be the last resort in case the locals cannot contact other possible Alerting Entities within the state. The local **SHOULD NOT** go to FEMA if the request was denied by authorized Alerting Authorities within the state.



AUTHORITY / REGULATION:

Public Law 114–143

114th Congress

Apr 11, 2016

The “Integrated Public Alert and
Warning System Modernization Act of 2015”.

Sec. 526.(c) SYSTEM REQUIREMENTS – The public alert and warning system shall:
(5) provide redundant alert mechanisms where practicable
so as to reach the greatest number of people;

In accordance with Public Law 114-143, The FEMA National Advisory Council (NAC), during its Feb 15, 2019 meeting, provided 14 recommendations to achieve the requirements of the Modernization Act of 2015. Recommendation 11 states:

“FEMA should develop the capacity and policy(s) for redundant alert origination capability to issue alerts at the request of alerting authorities or when they are unable to do so based on established standard operating procedure (SOPs) (e.g., delegation / succession of authority).”



To accomplish Recommendation 11, FEMA IPAWS has instituted the **Alert Escalation Process (AEP)** and the **Alert on Behalf (AOB)** process.

The **AEP** would be an internal state process whereby a local entity would allow another in-state entity to send an alert for them. The process would flow from the local entity up to the state (TDEM) if necessary.

The **AOB** would come into effect if the state could not send an alert for either a local entity or for the state. In this case, FEMA IPAWS would send the Alert on Behalf of Texas / TDEM.

The **AOB / AEP** process took effect on 23 Oct 2023. The effect of implementing it will require additional MOAs and Alerting Authorizations to be reviewed and approved by the TDEM IPAWS Coordinator / section. TDEM will also have to enter into an additional MOA and Alert Authorization with FEMA, to allow FEMA to send alerts on behalf of Texas / TDEM.



Missing and Endangered Persons Event Code Now Live

Overview

The FEMA Integrated Public Alert and Warning System (IPAWS), in collaboration with the Federal Communications Commission (FCC), introduces a new event code – the Missing and Endangered Persons (MEP) code. It allows state, local, tribal, and territorial authorities to send emergency alerts over television, radio, and cell phones to recover missing and endangered persons.

The MEP event code is for anyone who does not meet the criteria for an AMBER Alert, including children and adults. It supports a faster, more coordinated response from law enforcement and community members.



The MEP event code was created to fill the gap and help address the over 180,000 people who go missing annually that do not qualify for an AMBER Alert. It allows for quick and direct action because every second counts when someone goes missing.

The MEP event code can rapidly help mobilize public responses and equip rural and hard-to-reach areas for more resilient emergency communications for missing and endangered persons, which can provide lifesaving information quickly for communities that need it most.



OPSEC and SOPs

Define OPSEC

Protecting SOPs as part of OP SEC

I received a question from a local jurisdiction regarding whether their IPAWS – Alerting Procedures SOP should be a public or protected document. From a DHS OPSEC (Operational Security) standpoint, certain SOPs would fall under the Critical Information (CI) category, requiring some protection. This is information that is unclassified but requires protection / controlled dissemination.

The attached power point provides some slides from the DHS OPSEC course.

Since IPAWS is a federal program, I reached out to FEMA IPAWS for their input. FEMA IPAWS concurred with the Practice of protecting IPAWS SOPs.

This recommendation would not prevent the sharing of an SOP from legal actions but advises against placing the SOP on an open / public facing website.



History and Importance of OPSEC:

Operations Security (OPSEC) is a concept that is as old as early ancient tribal mankind. Through history, tribal societies have sought to win tactical or economic advantage over its rivals in order to gain power or overcome their security at all levels. Modern nations face the same challenges as their adversaries seek to gain information that can be used to defeat or compromise their security and national interests.

Current OPSEC concepts and procedures grew out of the U. S. Government commission dubbed the "**Purple Dragon Study**" in the late 1960s. The study team reviewed time tested principles and best practices in identifying critical and sensitive information that could reveal vulnerabilities in a wide range of government operations. Most weaknesses created by poor OPSEC were found to be the result of failure to identify and protect seemingly unimportant information that could unwittingly compromise the mission. From these findings, President Reagan signed National Security Decision Directive (NSDD) 298, which remains in effect today. NSDD 298 established OPSEC standards throughout the government to ensure that all **unclassified** information related to national security efforts would be reviewed prior to release or otherwise identified and protected.

Although security programs and procedures already existed to protect classified

[Back](#)[Next](#)

Review the terms listed below. Click on a term again to hide it.

1. Critical Information

Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

2. Adversary

Anyone who contends with, opposes, or acts against your interest and must be denied critical information.

3. Threat

An adversary with intent and capability to target, collect, analyze, and employ intelligence to act against friendly assets and activity.

4. Indicator

Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

▶ 0:09 / 0:09 - 🔊 ⋮

OPSEC Basic Awareness

employ intelligence to act against friendly assets and activity.

4. Indicator

Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

5. Vulnerability

A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making.

6. Risk

A measure of the potential degree to which protected information is subject to loss through an adversary.

7. Countermeasure

Methods and means to gain and maintain essential secrecy about critical information.

▶ 0:09 / 0:09 - 🔊 ⋮

Home

Module 1 of 2

Page 17 of 18

◀ Back

Next ▶



Apply Countermeasures

- Changes in procedure
- Controlling dissemination
- Cover and deception
- Speed of execution
- Awareness training



▶ 0:11 / 0:11 - 🔊 ⋮

[Home](#)[Module 2 of 2](#)[Page 22 of 25](#)[Back](#)[Next](#)



PBS WARN

PBS WARN Website

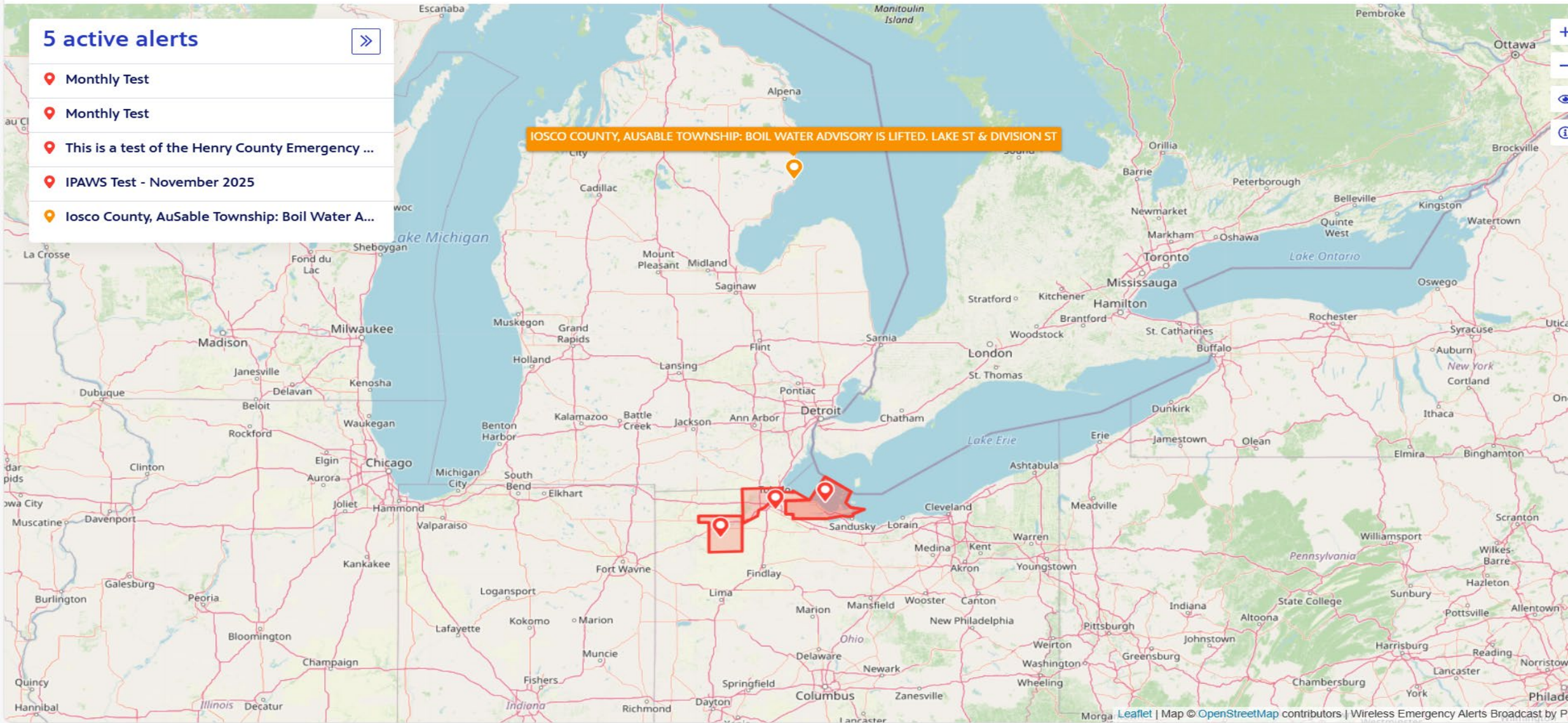
The PBS WARN website (warn.pbs.org) displays every Wireless Emergency Alert (WEA) issued in the United States and its territories. FEMA and public safety professionals across the US rely on The PBS WARN website for situational awareness and alert validation. They also use the PBS WARN website to search and display expired alerts for after-action reviews and training.



5 active alerts



- 📍 Monthly Test
- 📍 Monthly Test
- 📍 This is a test of the Henry County Emergency ...
- 📍 IPAWS Test - November 2025
- 📍 Iosco County, AuSable Township: Boil Water A...





WARN

Warning, Alert & Response Network

11:19:58 CDT
Updated 03/29/2025 11:19:28

Alert List



EVACUATION IMMEDIATE



MANDATORY EVACUATION

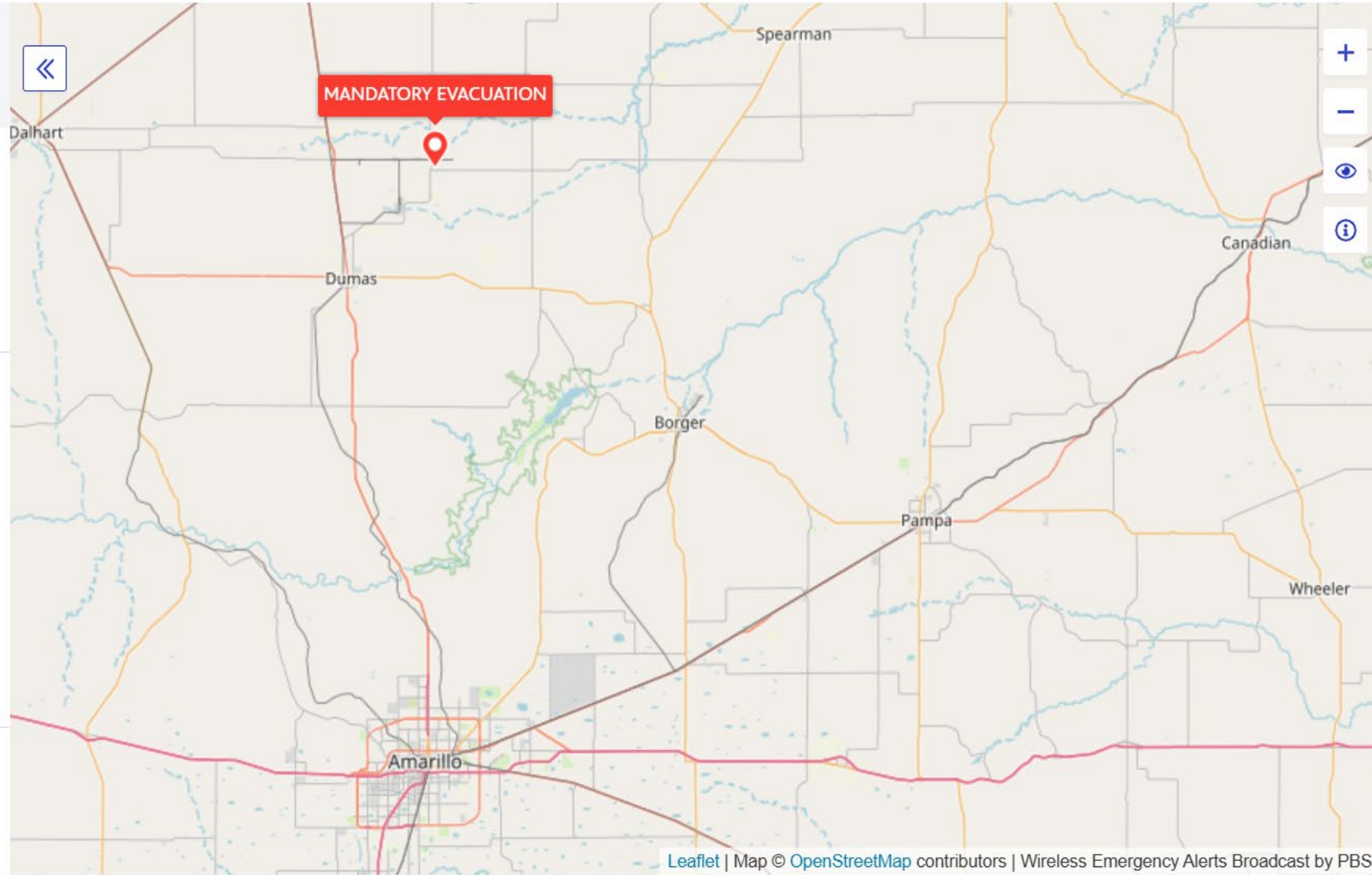
SENDER

PRPC,Amarillo,TX

EXPIRES

03/29/2025 11:47:26

↺ Carousel View



Leaflet | Map © OpenStreetMap contributors | Wireless Emergency Alerts Broadcast by PBS

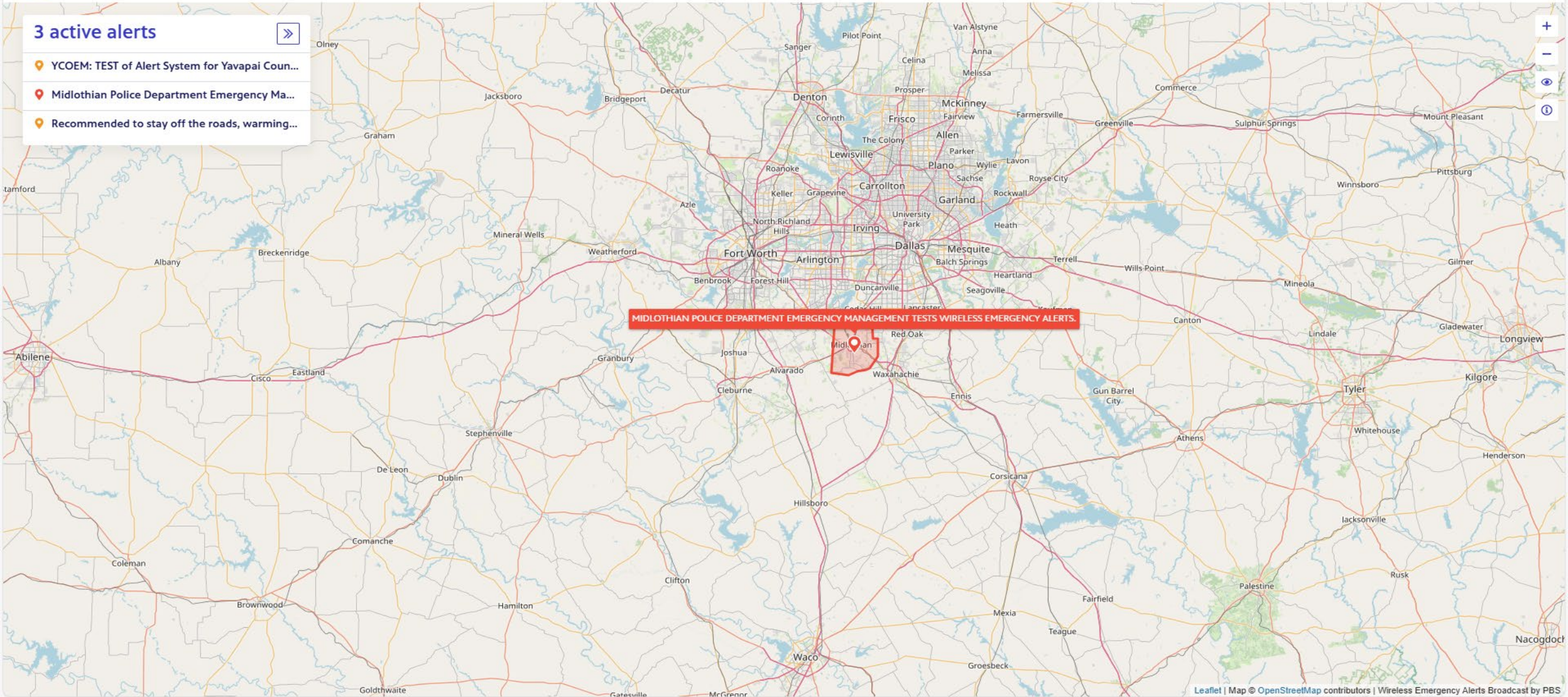


3 active alerts

YCOEM: TEST of Alert System for Yavapai Coun...

Midlothian Police Department Emergency Ma...

Recommended to stay off the roads, warming...



QUESTIONS ?

CODERED INCIDENT



TDEM IPAWS POC

Kevin Lemon

kevin.lemon@tdem.Texas.gov

Cell: (512) 203-0146

FEMA IPAWS Contact Info

<https://www.fema.gov/ipaws>

Contact the IPAWS Program Management Office at
ipaws@fema.dhs.gov

