WA-PAWS – Tab B6	**Alerting Procedures With IPAWS**	01.10.22

Signing Up to Use IPAWS to Send Public Alerts and Warnings

A federal, state, local, tribal or territorial alerting authority that applies for authorization to use the Integrated Public Alert and Warning System (IPAWS) is designated as a **Collaborative Operating Group or "COG."** Before beginning the below process, consult with the Emergency Management Division's Alert & Warning Center Supervisor, who is the State IPAWS representative (see Tab B2), for your ability to become an IPAWS alerting authority.

Step #1 – Complete IPAWS Web-Based Training

FEMA's Emergency Management Institute (EMI) offers the independent study course, IS-247 Integrated Public Alert and Warning System for Alert Originators. The goal of the course is to provide authorized public safety officials with:

- Increased awareness of the benefits of using IPAWS for effective alerts and warnings
- Improved skills to draft more appropriate, effective, and accessible alert and warning messages
- Increased understanding of the importance of training, testing and exercising with IPAWS
- Best practices in the effective use of IPAWS to reach members of the public

The course is a prerequisite for full access to IPAWS-OPEN for the purpose of public alerting.
Additionally, EMI offers the optional course, IS-251 Integrated Public Alert and Warning System for Alerting Administrators. The goal of the course is to provide authorized alerting administrators guidance with:

- Developing effective policies, plans and procedures
- Defining the approval process
- Defining the importance of training, practice and exercising with IPAWS
- Illustrating best practices and effective use of IPAWS to reach members of the public

Step #2 – Select IPAWS Compatible Software

To send a message using IPAWS, an organization must procure its own IPAWS-compatible software. View a **list of Alert Origination Software Providers** that have successfully demonstrated their IPAWS capabilities. FEMA does not provide training on third-party alert origination software. Contact your vendor for any software support questions.

Step #3 – Apply for a Memorandum of Agreement with FEMA

To become a COG, a Memorandum of Agreement (MOA) must be executed between the sponsoring organization and FEMA. The MOA governs interoperability and security across emergency response organizations and systems. Each MOA is tailored to the sponsoring organization and their interoperable software system.

To apply for IPAWS access, please send an email, with the subject line "COG Application." FEMA will then provide you with an application form and instructions to begin the process. Once the complete

MOA Application has been received by IPAWS, the Customer Support Branch will prepare the MOA for signature and return it to the sponsoring organization with a COG Identification (ID) number.

Beware: In accordance with the DHS Sensitive Systems Policy Directive 4300A, IPAWS MOAs have a lifespan of three years. After three years, the MOA must be renewed. Additionally, anytime personnel listed in the MOA or their contact information changes, the MOA must be renewed. New personnel must complete the training listed in Step #1 above, as a prerequisite for MOA renewal. The renewal of the MOA is the responsibility of the state, local, tribal or territorial alerting authority. Contact the Emergency Management Division's Alert & Warning Center Supervisor (see Tab B2) for assistance with MOA expiration and renewal.

Step #4 – Apply for Public Alerting Permissions

Alerting authorities that intend to send alerts to the public through IPAWS must complete an application defining the types of alerts they intend to issue and the extent of their geographic warning area. The application for IPAWS Public Alerting Authority (PAA) permissions will be provided when you apply for a COG MOA. In order to ensure consistency with state, tribal and territorial public alerting plans, the application must be reviewed and signed by the Emergency Management Division's Alert & Warning Center Supervisor, who is the State IPAWS representative (see Tab B2), before it is submitted to FEMA.

Beware: It behooves state and local alerting authorities to review their PAA permissions periodically as new dissemination channels and event codes become available over time and changes are made in the authorized use of event codes. Contact the Emergency Management Division's Alert & Warning Center Supervisor (see Tab B2) for assistance with PAA permissions review.

What to Expect

A copy of the executed MOA will be returned to the sponsoring organization along with a digital certificate that is needed to configure the IPAWS compatible software system. Once the public alerting application is received, specific alerting permissions will be implemented in IPAWS-OPEN. At that point the individual members, specified by the COG, will be able to send public alerts and warnings in their geographically prescribed areas.

Initial functionality includes the ability to access and send alerts through:

- the Emergency Alert System
- Wireless Emergency Alerts
- Non-Weather Emergency Messages

Beware: In accordance with the DHS Sensitive Systems Policy Directive 4300A, IPAWS digital certificates also have a lifespan of three years. However, the FEMA IPAWS Program Office will automatically issue a new digital certificate after three years if the alerting authority has met the Mandatory Monthly Proficiency Demonstration Requirement described below.

Testing IPAWS Alert and Warning Dissemination

The IPAWS Technical Support Services Facility (TSSF, formerly known as the IPAWS Lab) is a secure, closed practice and training environment capable of demonstrating alert dissemination to all IPAWS

pathways such as the Emergency Alert System, Wireless Emergency Alerts, and Non-Weather Emergency Messages.

The IPAWS TSSF enables public safety officials to gain confidence using IPAWS in this practice and training environment without disseminating messages to broadcasters and the public. Additional purposes of the IPAWS TSSF include alert and warning, functional assessments, alert dissemination validation, training, procedural and process evaluation, and to establish functional requirements.

To access the IPAWS TSSF closed training and demonstration environment, an Alerting Authority must possess a demonstration digital certificate and ensure that its IPAWS-capable alert origination Each COG is required to ensure software is directed to the IPAWS TSSF URL: https://demo.integration.aws.fema.gov/IPAWS_CAPService/IPAWS. Most software vendors manage this requirement for their clients.

The IPAWS Program Office has implemented a Mandatory Monthly Proficiency Demonstration Requirement. **IMPORTANT** - Each authorized alerting authority must demonstrate their ability to compose and send a message through the IPAWS-OPEN system at least once a month.

- **Live messages sent to the production environment WILL NOT be considered for Monthly Proficiency Demonstration scoring.**
- **If a COG misses a single Monthly Proficiency Demo, they will receive a reminder from FEMA.**
- **If a COG misses two consecutive Monthly Proficiency Demos both they and the Emergency Management Division's Alert & Warning Center Supervisor, who is the State IPAWS representative (see Tab B2), will be notified.**
- **If a COG misses three consecutive Monthly Proficiency Demos they will lose access to the IPAWS Live Production Environment and not be able to use IPAWS for public alerting until such a time as they complete a successful Monthly Proficiency Demo.**

IPAWS Alerting Procedures

The state as well as most counties in Washington use IPAWS-compliant software to disseminate public alert and warning messages through IPAWS following jurisdictional warning procedures. Jurisdictions are free in the choice of their software.

Although IPAWS-compliant software functionality may vary slightly from vendor to vendor, some the common functionality includes:

- Simultaneous generation of EAS, WEA, and NWEM messages
- Simultaneous launch of English and Spanish message versions
- Definition of target areas by FIPS codes or polygons
- Use of message templates and pre-scripted messages
- Origination of live alerts and warnings to the public as well as test alerts and warnings to the IPAWS TSSF

The nature and extent of the threat will determine whether the state or the local jurisdiction will originate a given alert, recognizing that local jurisdictions are in the best position to include pertinent protective action recommendations with the alert.

Jurisdictional Alert, Warning, and Notification (AWN) Plans
For the purpose of effective EAS message dissemination, multi-county local operational areas have been defined based on the existence and availability of broadcast media in the area (see Tab B9). Tab D3 provides links to the Local Operational Area Plans.

Best practice: Alerting authorities should develop comprehensive jurisdictional alert, warning, and notification (AWN) plans including all systems and technologies in use.

Plans, policies, and procedures should define roles and responsibilities including identifying who can request, approve, and disseminate an AWN, how to select an appropriate system for an AWN dissemination, and what to do in the event of an incorrect or false message issuance. Plans, policies, and procedures should be well-documented, supplemented with any necessary additional guidance, field-tested, consistently evaluated for potential gaps and updated accordingly, able to dynamically adapt as the AWN landscape and technologies evolve, based on community threats and hazards, and integrated into operations. These frameworks reduce AWN issuance delays and prevent inconsistencies, by outlining coordination structures between alert originators within a jurisdiction and neighboring jurisdictions, roles and responsibilities, system utilization scope and expectations, and the steps required for carrying out time sensitive and essential tasks.

Resources:
Developing an AWN Program Plan | FEMA.gov
Public Safety Communications: Ten Keys to Improving Emergency Alerts, Warnings, and Notifications | CISA