Statewide Guidance on Alerts, Warnings, and Notifications

October 2022

STATEWIDE INTEROPERABILITY

Interoperability begins with relationships.

OREGON DEPARTMENT OF EMERGENCY MANAGEMENT
OEM

This page left blank intentionally.

Table of Contents

Letter from the Statewide Interoperability Coordinator

"Never underestimate the power of a small group of committed people to change the world. In fact, it is the only thing that ever has." ~ Margaret Mead

In 2019, the State Interoperability Executive Council adopted an objective in the State Communications Interoperability Plan to improve public emergency alerts and warnings throughout the state. As a result of this effort, the OR-Alert Program was authorized by the Oregon Legislature and created within the Statewide Interoperability Program. OR-Alert's mission is to:

> *"Ensure access to timely and informative alerts, warnings, and notifications (AWNs) through implementation of a statewide system that enables state, county, city, and tribal governments to issue AWNs—**providing people in Oregon with meaningful opportunities to make life-saving decisions in the face of emergencies"***

Since its inception, the tools that make up OR-Alert have been used more than 3,000 times to alert people in Oregon to life threatening hazards, including wildfires, flooding, acts of violence, hazardous weather, heat emergencies, and other incidents. OR-Alert currently has contact information for over 3.7 million of Oregon's 4.1 million residents. 21 statewide templates have been developed and professionally translated into Spanish, reviewed for cultural competency and accessibility, and distributed across the enterprise, with an additional nine templates developed for regional events. These templates make it easier for system users to quickly send alerts with clear and consistent messaging.

Beyond the tool, OR-Alert was created based on the idea that we are better when we work together. The business of public alert and warning is and must always be a team effort. OR-Alert is governed by a diverse committee made up of emergency managers, public safety leaders, state agency and tribal representatives, and other stakeholders from across the state, and from across all levels of government who share a vision of saving lives through timely alerts, warnings, and notifications. It is this collaborative governance model that makes Oregon and the OR-Alert Program so unique and effective. On behalf of this amazing group of public servants, and with grateful acknowledgment of the assistance provided by the Cybersecurity and Infrastructure Security Agency's Interoperable Communications Technical Assistance Program, I am pleased to present Oregon's Statewide Guidance on Alerts, Warnings, and Notifications.

William Chapman
Statewide Interoperability Coordinator

Document Revision Process

The Oregon Alerts, Warnings and Notifications guidelines are reviewed at a minimum, every two (2) years. The OR-Alert Governance Committee, the Oregon Department of Emergency Management, and the Statewide Interoperability Coordinator (SWIC) are responsible for conducting the review. Time critical updates may be initiated at any time and submitted using this same process. Any updates or changes to this document are submitted to the OR-Alert Governance Committee for approval prior to implementation.

Once approved, all changes to the document are recorded in the Revision Record.

Revision Record

VERSION	DATE	DESCRIPTION OF CHANGE

Purpose

This document provides guidance on the use of Federal Emergency Management Agency's (FEMA) Integrated Public Alert and Warning System (IPAWS) and the processes and procedures for issuing alerts, warnings, and notifications through the State of Oregon's OR-Alert system. The OR-Alert system includes several tools that emergency managers can use to reach different segments of the population, depending on the scope and scale of the emergency. OR-Alert includes:

- A mass notification tool capable of issuing geotargeted messaging to contacts via a wide array of communications modalities including text message, email, and voice call
- Mobile App based messaging
- Keyword based messaging
- IPAWS messaging
- Automated National Weather Service messaging

This guidance is designed to help ensure that the citizens and visitors of Oregon are notified of life-threatening situations in as timely and accurate manner as possible.

The Oregon IPAWS administrator establishes the codes alerting authorities are permitted to use, approves Collaborative Operating Groups (COG) for certification, and approves testing procedures and events for Wireless Emergency Alerts (WEA) broadcast testing.

Administration

The State IPAWS Administrator is housed within the Oregon Department of Emergency Management (OEM). OEM is responsible for working with FEMA to grant credentials for use of IPAWS.

The OR-Alert Program is administered by the Statewide Interoperability Program within Enterprise Information Services. The Program manages access and use of the OR-Alert system in collaboration with the OR-Alert Governance Committee.

This document discusses Emergency Alerting System (EAS) processes; however, the official EAS Plan is contained in a different document created by the State Emergency Communications Council (SECC) and approved by the Federal Communications Commission (FCC). Further explanation is contained in this document.

Section 1: What are Public Alerts, Warnings, and Notifications?

A public **alert** is a communication intended to alert the public and direct their attention to an immediate, occurring risk or hazard. They occur at the beginning of and during incidents with an ongoing, immediate threat. Alerts may also include instructions for potential protective actions and provide ongoing communications relevant to an event. The measure of an effective alert message is the extent to which the intended audience becomes attentive and seeks further information.

A public **warning** is a communication intended to notify the public of an imminent event and to persuade them to take one or more protective actions to reduce losses or harm. The measure of an effective public warning message is the extent to which the intended audience receives the message and takes the protective action and/or heeds the guidance.

Notifications include **public** and **internal** notifications. These notifications/advisories are not to be used for promoting public or private events.

- **Public** notifications/advisories can include protective actions, evacuation routes, boil water advisories, traffic advisories and return from evacuation notices.
- **Internal** notifications/advisories provide communications and information as defined by the agency.

Type	Timeframe	Purpose	Examples
Alerts	At the beginning of and during incidents with an ongoing, immediate threat	Gain the attention of the public and draw their attention to a risk or hazards	Active Shooter and other civil dangers, hazardous materials (HAZMAT) concerns, 911 Outages, AMBER Alerts, etc.
Warnings	Prior to incidents	Distribute guidance to prepare for an anticipated incident	Weather watches /warnings, fire warnings, flood warnings, volcano warnings, evacuation orders
Notifications	During and after immediate threats; also includes non-event related messaging	Instruct protective actions and provide ongoing communications relevant to an event. Convey time sensitive information on response and recovery related services	Evacuation routes, boil water advisories, return from evacuation notices, area accessibility updates, all clear notices

Section 2: Roles and Responsibilities

Planning for, preparing, and disseminating alerts and warnings is the responsibility of multiple levels of government. Each level of government—and designated entities within those levels—hold responsibility and/or authority to ensure the overall effectiveness of alerts, warnings, and notifications within Oregon.

Local Jurisdictions (Counties and Tribes)

All disasters and emergencies are locally oriented. Depending on how the local area governments - organized and coordinated the local area alert and warning system, the local government responsibility can be inclusive of city, special district, county, and multi-county jurisdictions. While first responders are preparing to respond to the initial after-effects of an incident, it is an inherent responsibility of local officials to keep the public informed of what actions the public needs to take to protect themselves and their families.

Communicating these instructions to public audiences is the primary purpose of OR-Alert. Because local officials have a better understanding of the situation, the immediate actions that are being taken, and potential adverse impacts of the incident, it is incumbent upon them to communicate to the public rapidly and effectively what is going on and what needs to be done to potentially save lives.

These actions may include but are not limited to:

- Evacuation orders (Including evacuation routes, shelter info, key information, etc.)
- Locations of points of distribution (for food, water, medicine, etc.)
- Direction to move to higher ground
- HAZMAT incidents
- Red Flag warnings
- Weather alerts
- Lockdown
- Shelter-in-place guidance

To successfully accomplish this task, local jurisdictions must have a structure in place to provide for rapid alerts and warnings. Local jurisdictions are responsible for:

- Operating the OR-Alert platform for the dissemination of messaging related to local events.
- Developing and submitting to the State, a standard operating procedure or policy that identifies emergency notification processes and procedures and points of contacts which includes procedures for initiating, cancelling, and rescinding accidental alerts, and for rapidly correcting and updating alert details as additional information becomes available.
- Drafting alert templates for commonly encountered emergencies.

- Understanding how limited telecommunications infrastructure and network congestion may affect alerts and warnings in the community.
- Ensuring alert originators are properly trained on how and when to utilize the system.
- Identifying who will originate an alert.
- Developing message approval processes.
- Identifying trigger points for emergency alerts.
- Designating in writing, in accordance with the FEMA application process, no fewer than three individuals who will be the jurisdiction's alerting authorities for issuing emergency alerts. (Typically, this would be the jurisdiction's emergency manager, staff and/or 9-1-1 or Dispatch Center staff.)
- Incorporating OR-Alert into existing and future response plans and procedures as well as training and exercise events.
- Participating as part of the OR-Alert Governance Committee at least biannually.
- Enactment of ordinances and/or policies identifying local roles and responsibilities to enable the issuance and coordinated dissemination of alerts and warnings to the public by responsible officials within their jurisdictions regarding imminent threats to human life and health and extraordinary threats to property.
- Installation, maintenance, user training, and exercise/testing of local jurisdiction specific public alert and warning capabilities within their jurisdiction (e.g., tsunami warning sirens).
- Understanding the access and functional[1] needs-related considerations associated with public alert and warning systems and messaging. To fully understand these considerations, jurisdictions should:
    1. Have systems in place to identify the strengths and needs of access and functional needs communities.
    2. Develop plans to build on strengths while addressing identified needs.

[1] "Access and functional needs" refers to individuals with and without disabilities, who may need additional assistance because of any condition (temporary or permanent) that may limit their ability to act in an emergency. Individuals with "access and functional needs" do not require any kind of diagnosis or specific evaluation. These may include but are not limited to

- individuals with disabilities,
- individuals with limited English proficiency,
- individuals with limited access to transportation,
- individuals with limited access to financial resources,
- older adults
- others deemed "at risk" by the Pandemic and All-Hazards Preparedness and Advancing Innovation Act (PAHPAIA) or the Secretary of Health and Human Services.

- Participate in revisions of mandated FCC local EAS plans, including approval of authorized event codes.
- Coordinate with adjoining jurisdictions, and the State regarding origination of alerts and warnings related to hazards that have effects across jurisdictional boundaries.
- Maintain security and authorized access to their systems.
- Comply with the requirements outlined in the OR-Alert Intergovernmental Agreement.
- Provide a single point of contact to the OR-Alert Program for system administration and participation in the OR-Alert Governance Committee.

In general, only one (1) Public Alerting Authority (PAA) will be authorized per County/Tribe. Consideration will be given to include military installations and other large, contained campus type installations on a case-by-case basis. This consideration will be given in coordination with the local Primary Public Alerting Authority. This restriction does not preclude the Public Alerting Authority from collaborating with additional agencies and organizations within the jurisdiction. The PAA is encouraged to approach emergency alerting from an all-hazards perspective and be inclusive of all partners.

State

Recognizing that all disasters are local, the primary responsibility of the State is to facilitate the implementation of IPAWS into the emergency notification network and to maintain the OR-Alert Program. In the case of a catastrophic local, state, r regionally defined event, the State will provide a resilient and comprehensive alert and notification capability. These responsibilities fall across multiple state agencies The following sections outline who is responsible for what within the State.

The Oregon Department of Emergency Management

The Oregon Department of Emergency Management:

- Provides IPAWS warnings and other alerts on behalf of county agencies and/or state agencies when requested and authorized as necessary.
- Maintains situational awareness of alerting activities across the State.
- Serves as an advisory member to the OR-Alert Governance Committee.
- Administers the State's role in the IPAWS application process by:
    - Reviewing and approving, as deemed necessary, applications for COGs for all local and state agencies.
    - Conducting monthly tests of the system to ensure functionality of equipment and the network as required by FEMA.

The Statewide Interoperability Program

The Statewide Interoperability Program (SWIP):

- Administers the OR-Alert system.

- Manages the OR-Alert contract and vendor.
- Performs audits of the system to ensure functionality of the system and adherence to established policies and procedures by system users.
- Supports governance of the OR-Alert system.

Together, the Statewide Interoperability Program and the Oregon Department of Emergency Management have agreed to:

- Encourage proliferation of the OR-Alert System to all eligible entities within the State.
- Encourage subscriber opt-ins to local systems.
- Assist the OR-Alert Governance Committee with development of alerts, warnings, and notification best practices for use within Oregon.
- Maintain www.ORAlert.Gov.
- Participate in after action reviews and "Hotwashes" regarding system use after an incident, emergency, or planned event.
- Evaluate proposals for added functionality of the system in consultation with the Governance Committee.

Oregon State Police

The Oregon State Police (OSP) is responsible for statewide coordination of Oregon's *America's Missing: Broadcast Emergency Response* (AMBER) Alerts on behalf of Oregon law enforcement agencies. This mission is accomplished through the OSP Northern Command Center (NCC).

In conjunction with the law enforcement agencies initiating a request for an AMBER Alert, the OSP NCC coordinates the statewide initialization of an AMBER Alert utilizing OR-Alert. Additionally, the OSP NCC serves critical support functions in a wide variety of areas, including coordinating the activation of the Variable Message Signs (VMS) system on Oregon's highways. To request assistance, agencies should call the OSP NCC at 1-866-290-1863.

The OSP NCC utilizes OR-Alert to notify the many AMBER Alert partners (i.e., Oregon Lottery, Oregon State Library network).

OSP NCC contacts Oregon State Police Criminal Investigation Division (CID) for all AMBER Alert activation requests. CID supports local law enforcement and the AMBER Alert program with immediate resources such as a fully staffed Tip Center, the State's Missing Children's Clearinghouse, as well as access to crime analysts, and major crime investigators statewide.

Federal

National Oceanic and Atmospheric Administration

The National Oceanic and Atmospheric Administration (NOAA) through the National Weather Service (NWS) is responsible for originating public warnings regarding weather hazards. The NWS operates several public alert and warning

dissemination systems, including the NOAA Weather Radio (NWR), a network of over 1,000 VHF radio transmitters serving the population of the United States. NWR is an “All Hazards” radio network, making it a single source for comprehensive weather and emergency information. In conjunction with Federal, State, and Local Emergency Managers and other public officials, NWR also broadcasts/conveys warning and post- event information for all types of non-weather hazards – including natural (such as earthquakes or avalanches), environmental (such as chemical releases or oil spills), and public safety (such as civil emergency messages or 9-1-1 telephone outages).

NOAA also operates the NOAA Weather Wire Service (NWWS), which provides television and radio broadcasters, emergency managers, commercial / private alerting services, and the general public the fastest receipt of current weather information, distributed as alerts and warnings sent in text format from the local NWS Weather Forecast Offices and National Centers. Additionally, the NWS operates the Emergency Managers Weather Information Network (EMWIN), a system developed to provide emergency managers, public alerting services, and the public at large quick and free access to a defined set of NWS warnings, watches, forecasts, and other products.

Finally, the NWS National Tsunami Warning Center issues Tsunami statements, watches and warnings which are disseminated by the Coastal NWS offices.

While NOAA through the NWS is responsible for weather related alerting, local government is not precluded from sending notifications and alerts in support of weather events.

FCC

The FCC, in conjunction with FEMA and NOAA NWS, implements the Emergency Alert System (EAS) at the federal level. The FCC's role includes establishing technical standards for EAS participants, procedures for EAS participants to follow in the event the system is activated and testing protocols for EAS participants.

FEMA

FEMA maintains and operates IPAWS. IPAWS is FEMA's national system for local alerting that provides authenticated emergency and life-saving information to the public through mobile phones using WEA, to radio and television via the EAS, and on NOAA’s Weather Radio. IPAWS was established under Executive Order 13407. IPAWS provides the capability to notify the public of impending natural and human-made disasters, emergency, and public safety information. In a national emergency, the President may use IPAWS to communicate to the public as well. IPAWS delivers timely, geographically targeted messages during emergencies to save lives and protect property.

FEMA provides 24/7 technical support for IPAWS users and is responsible for issuing credentials for use of the system through OR-Alert.

OR-Alert Governance Committee

OR-Alert Governance Committee

The OR-Alert Governance Committee is comprised of organizations with life safety missions (e.g., Counties, Tribes, OEM, OSP), organizations with information only missions (e.g., ODOT), and advisory organizations (e.g., the Public Utility Commission (PUC), telecommunications providers, and others). The Committee provides input on statewide governance of alerts and warnings, and the OR-Alert Program to better serve Counties, Tribes, State Agencies, OEM, the Statewide Interoperability Program, and individuals throughout the state of Oregon. The Committee is responsible for defining "best practices" and guidelines for alerts, warnings, and notifications throughout the state.

The vision of the OR-Alert Governance Committee is to "Establish equitable access to a statewide system that enables state, county, local, and tribal governments to issue timely, informative alerts, warnings, and notifications."

The mission of the OR-Alert Governance Committee is "To ensure access to timely and informative alerts, warnings, and notifications (AWNs) through implementation of a statewide system that enables state, county, city and tribal governments to issue AWNs—providing people in Oregon with meaningful opportunities to make life-saving decisions in the face of emergencies."

The Committee's primary goals and objectives are as follows:

- Advise OEM and Statewide Interoperability on best practices regarding implementation of OR-Alert.
- Encourage county, state agency, and tribal participation in OR-Alert governance, policy, and operations development.
- Encourage public adoption and participation in OR-Alert via local systems.
- Provide Subject Matter Expertise in reviewing After Action Reviews (AARs) related to AWN issued.
- Encourage adoption of best practices that integrate equity considerations into alert and warning systems. These should ensure accessible, culturally, and linguistically appropriate, equitable and timely communication.

The OR-Alert Governance Committee shall be made up of representatives of the following:

- Oregon Department of Emergency Management
- Statewide Interoperability Program
- State Interoperability Executive Council
- PUC
- OR-Alert system Administrators
- Emergency Communications Centers (PSAPs)
- Oregon Association of Broadcasters (OAB)
- NWS local weather forecast offices

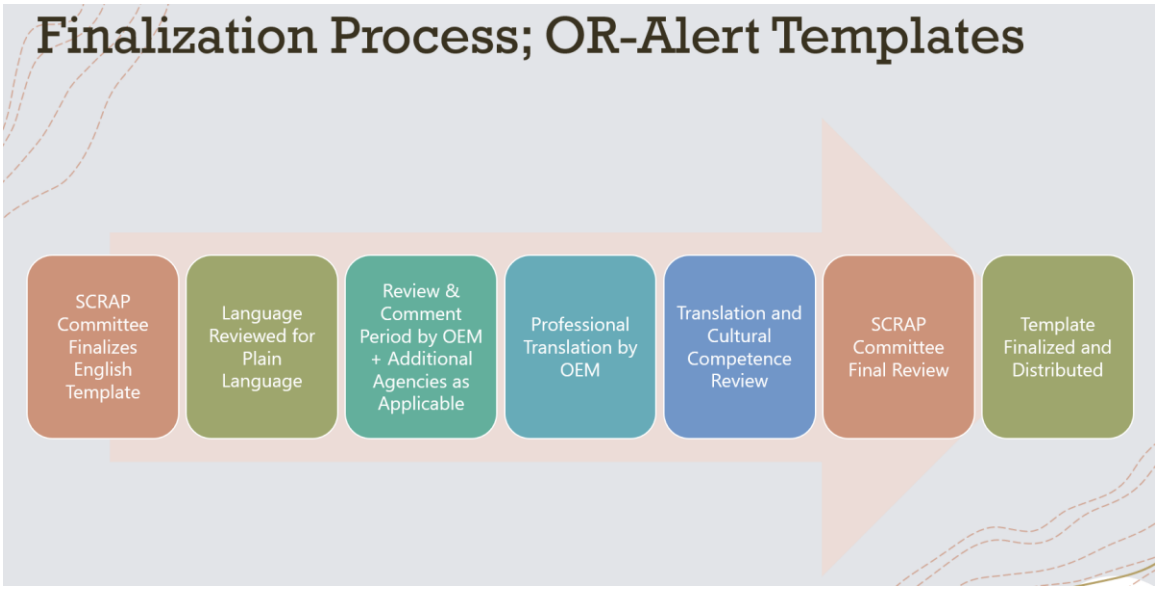
- Representatives from commercial telecommunications providers
- Community Based Organizations

The OR-Alert Governance Committee Charter is available online here.

Sub-Committee on Recommendations for Alerting Practices (S.C.R.A.P)

The Sub-Committee for Recommendations on Alerting Practices (SCRAP) is a sub-committee of the OR-Alert Governance Committee. Membership is open to county/local emergency managers, state agency representatives, community-based organizations/non-profits, emergency communications center (PSAP) personnel, and others. The objective of committee members is to act as a liaison for State, County, Local and Tribal Government needs, to collaboratively develop effective messaging templates, to maximize limited internal resources, to promote a shared understanding of best practices for alerts and warnings, and testing and exercises. The goal is to work together for continual improvement.

The SCRAP committee will identify common emergencies and develop standardized alert and warning templates for state-wide distribution. The template creation and finalization process are depicted in the chart below.



.

Section 3: Technologies

Integrated Public Alert and Warning System (IPAWS)

IPAWS is an internet-based capability, administered by FEMA, which Federal, State, Local, Tribal, and Territorial authorities can use to issue critical public alerts and warnings. The three core components of IPAWS are EAS, WEA, and NOAA Weather Radio. IPAWS also includes capabilities for unique alert systems, which includes dissemination of alerts through third party applications, and future system development.

IPAWS is an emergency alerting tool, that can be used by local authorities for sending local emergency alerts. Each approved PAA can issue IPAWS alerts through OR-Alert. Each PAA is assigned one or more Federal Information Processing Standards (FIPS) codes for Non-Weather Emergency Messages (NWEM) and EAS activations. The alert is disseminated to the entire county, or in the case of WEAs, to a smaller geotargeted area as defined by the alert originator.

IPAWS is a “system of systems” that can use the following additional alerting dissemination methods and technologies. Alerting authorities should consider the following when composing and issuing alerts:

Emergency Alert System (EAS)

The EAS broadcasts alerts through radio and television stations in the area. The alerts may or may not be automatically broadcasted from a local alerting authority depending on the alerting preferences set by the broadcaster, as identified in the Oregon EAS Plan. Additionally, EAS enables the President of the United States (POTUS) to interrupt all broadcasts in one or more counties with an emergency announcement. Participation in local use of EAS is voluntary on the part of broadcasters except the Local Primary LP-1 and LP-2 stations. EAS messages are delivered to all listeners or viewers of stations serving a targeted county. Satellite and cable TV carriers also participate in EAS, but their capacity to geographically target dissemination is more limited. EAS can distribute warning messages over large areas very quickly but cannot reach people who are not watching or listening to broadcast media, particularly people who are asleep. Some individuals may need assistive technology to access these alert systems, and the language groups served by the broadcast agencies of the EAS may not evenly support all needed language groups in a geographic area. Further information regarding EAS issuance can be found in the Oregon EAS Plan created and maintained by the SECC. The SECC consists of the NWS, OEM, and broadcasting infrastructure representatives.

Wireless Emergency Alerts

WEAs are emergency messages sent by authorized government alerting authorities through mobile carriers. They broadcast a text alert to all WEA capable cell phones within the designated alerting area. WEAs are very brief

messages, limited to 90 or 360 characters. WEA alerts are targeted to a defined geographical area and are presented differently than a typical text alert to differentiate it from regular notifications. They offer a unique alert tone and vibration accompanied by a brief push notification displayed on the end user's mobile device. Mobile device users will receive the WEA notification unless they choose to deactivate the service on their mobile device. The targeted area may not completely match a polygon or area selected through the OR-Alert mapping interface due to how the cellular carriers choose to deliver the messages. Cellular carriers may "overshoot" an area to guarantee at least 99% of people in the polygon receive the message.

Mistargeting of WEAs by Cellular Providers

Extreme overshooting or mistargeting of an area during the issuance of a WEA can undermine alert originators' ability to message the public effectively and may lead to recipients ignoring messages. Reports of messages received 10 or more miles outside the polygon or reports of not receiving a message when inside the polygon should be reported to the SWIP for follow up with the carriers. Reports may be made by sending an email to OR.Alert@das.oregon.gov with the following information:

- Date/Time of message issuance
- Message topic (Wildfire, weather, other)
- Carrier
- Location of where the alert was (or was not) received, in as much detail as possible so the carrier can plot the polygon, circle or FIPS code against their coverage and site locations
- Device model, operating system, and telephone number of device(s) affected

Emergency Mass Notification Software Systems

Many localities can call telephone numbers in an organizational database and play an audio message. These systems draw from opt-in data and publicly accessible "white" and "yellow" pages like databases provided through the OR-Alert Program. Another advantage of these systems is their ability to precisely target a message in a specific geographic area.

Telephonic notification systems can provide extensive warning information. The amount of time to execute all the calls; however, can be limited by the local telephone infrastructure, length of the verbal message, or limits to the technology initiating the calls. Alerting authorities at the local and county level have an obligation to work with local telecommunications providers to understand these limitations and throttle their message delivery appropriately to ensure that messages are successfully delivered to recipients.

Based on system settings, the system may automatically leave a message for telephone recipients who do not answer. However, the message sender may also opt to include the voice recording on an Audio Bulletin board; meaning

recipients may call the number back on their caller ID to access the message. It is recommended that alerting authorities make use of both features to ensure the best possible chance of a recipient receiving the message.

Finally, these systems can use a variety of other communication mediums including Short Message Service (SMS) and Short Message Peer-to-Peer (SMPP) text messages, emails, fax, telecommunications device for the deaf (TDD)/teletypewriter (TTY), and others. It is recommended that when sending a message, all contact methods are utilized and that the system be set to request confirmation of message receipt. This ensures the system will try and reach a contact via all possible methods until it receives positive confirmation that the contact has received the message.

Social Media

Social media is a critical component to disseminating emergency messaging, instructions, and recovery information to both the media and the public. Due to its unique nature, it functions instantaneously and creates highly visible official dialogue between the agency and very large groups of people, including news media and stakeholders. Messaging for social media must be very carefully managed. It has the capability to deliver text, audio, video, images, infographics, maps, and other data but requires a unique skill set and commitment to manage. These platforms have inherent expectations for two-way engagement with the public and therefore demand more staff time and resources.

Social media is more successful when the community is engaged and aware of accounts prior to a disaster. Social platforms may include:

- Facebook
- Instagram
- Twitter
- LinkedIn
- YouTube
- Others

Considerations and recommendations for incorporating social media into alert and warning before, during, and after emergencies include:

- Social media outreach is highly dependent on working cellular and data networks that may be impaired or offline during and following an emergency.
- Consider the variety of languages and the complexity of language to use in postings.

- Social media can be utilized as a dissemination resource capable of accommodating unthrottled traffic from the public without impacting traffic to locally hosted websites vital to local response.
- Social media is effective at reaching the news media, which may assist in more broadly sharing messaging.
- Briefings and updates via live and recorded video are recommended when internet access and bandwidth allow.
- Government agencies are required to allow public comments to be posted and seen to protect free speech. Two-way engagement is expected by the public.
- Dedicated staff resources are necessary to facilitate, manage, monitor, and analyze social media.
- Social media usage varies widely among different social, economic, and demographic groups.
- Information gleaned from social media analysis may not reflect a balanced or complete picture.
- Ensure messaging is consistent across all alerting platforms.
- Ensure there is a process in place to address reports of emergencies (imminent threats to health and welfare, reports of citizens trapped or injured and third-party reports of people in danger or a long period of non-contact) to all the previously mentioned social media platforms.

Anonymous Opt-In Systems

The OR-Alert program makes available a platform for people to opt-in anonymously via zip code or keyword, resulting in an increased number of alert and warning registrations, while also expediting the registration process. This system allows recipients to opt-in anonymously and quickly, and therefore helps to inform those who might not otherwise be interested in or aware of emergency alert programs. Community members can anonymously opt-in to zip code-based notifications (location specific information) or Keyword-based notifications (information related to a key word such as a wildfire event or county fair). Messages are not restricted to emergency notifications and can be used for community events. Use of these systems also allows third party alerts to receive and republish alerts to disseminate the message more widely. Current third-party integrations are:

- Google Public Alerts (Publishes alerts to the Google Homepage and via Google Maps)
- Ring Neighbors App (Publishes alerts to the Neighbors mobile app by Ring)

Unfortunately, recipients who opt-in in this manner are not tied to an individual geo-point, and as such, cannot be geo-targeted for location specific messages. Therefore, it is incumbent on message originators to be sure to include locations specific information in the message body.

These systems are most successful when:

- Keyword and zip code opt-in information is advertised as part of a rising incident, or in advance of planned events.
- Used to maintain engagement from incident awareness through recovery and support.

Considerations for incorporating these systems before, during, and after emergencies include:

- Imminent threat to life messages may be re-published by third party messengers, in effort to help spread life safety instructions.
- Messages may have character limitations.
- Keywords can be used continuously and/or reused while maintaining opt-ins.
- Zip code-based notifications cannot be distributed to geographic areas smaller than an entire zip code.
- Most of these systems allow Opt-Ins to unsubscribe by texting STOP.
- Reach of these systems are highly dependent on working cellular and data networks that may be impaired or down during and following an emergency.
- Two-way communication is not possible.
- Message receipt and delivery results are not provided.

Mobile Apps & Use of Geo-Fencing Alerting Products

Mobile apps are a critical component to disseminating information and accessing resources. OR-Alert members can push messages through mobile apps such as “ManageBridge”. Message recipients may receive messages through an alternate app such as the “Everbridge” mobile app. Mobile applications may enable notification scrolling including images, logos, hyperlinks and conference calling. Mobile apps also enable recipients to share messages and to engage in two-way communication by sharing location, images, or additional information with the message sender.

Further, mobile apps can extend the reach of notifications for people who have the app but are not subscribed to a local system (including travelers, tourists, and visitors). The use of a geofence to alert unsubscribed people of an incident can be effective. OR-Alert’s current vendor is Everbridge, who offers “Incident Zone” as a geofence alerting function used in conjunction with the mobile app. When shapes are used to depict a geographic incident boundary, the message sender

can choose to use the shape as a geo-fence. When the geofence/incident zone is enabled, anyone with the Everbridge mobile app and their locations turned on will receive the notification, provided their location crosses the perimeter of the incident zone within the broadcast duration.

Multi-Jurisdictional Awareness Through Networking of Systems

Keeping neighboring counties, agencies, tribes, and State partners aware of active incidents within a jurisdiction is key in enhancing exposure, maintaining awareness of potential threats and risks, and improving interoperability efforts. OR-Alert's current vendor, Everbridge, offers the Everbridge Network as a publishing option. Messages published to the Everbridge State of Oregon Network will provide a multi-jurisdictional view of incidents in the State of Oregon. If a polygon is published with the message, the network will depict the impacted area on a statewide map. Optional automatic email thresholds can be set up to notify OR-Alert members when an incident is posted.

Use of the State of Oregon Network is a key component of OR-Alert and ensures that cross jurisdictional alerting is enabled. Publishing to the network may also extend the reach of a message, as agencies with internal alerting systems may retransmit the alert to their own employees, volunteers, contractors, etc. thus ensuring these groups receive the message, even if not opted into the local system.

It is recommended that all alerts that may affect life safety be published to the State of Oregon Network. All statewide templates will include publishing to the state network as a default setting.

Section 4: Public Alerts and Warnings Best Practices

Events/incidents can evolve in extreme ways. Alerts, warnings, and notifications need to be an integral component of a jurisdiction's preparation for such events. Issuing public alerts, warnings, and notifications requires the exercise of reasonable and well-informed judgment. This action must be well practiced and familiar to the initiator when incidents dictate.

Best Practices

There is no all-encompassing formula for making messaging decisions. There are; however, some evidence-based principles and best practices that can help guide the decision maker:

- Utilization of alerting mechanisms within the IPAWS should be a primary route to issue emergency alerts and warnings to ensure the greatest number of recipients within the impacted area are being alerted.
- The responsibility for issuing alerts, and warnings during an emergency rest with designated public officials—known as PAA —at the county/state/tribal level. It is the choice of the PAA to determine who authorizes the issuance of alerts and/or warnings. It may differ from PAA to PAA.
- Unless otherwise notified, county emergency management agencies are generally considered to be the primary alerting authority for their jurisdiction.
- Messages should clearly identify the originating agency.
- Incomplete or imperfect information is not a valid reason to delay or avoid issuing a warning. Time is of the essence, as recipients of warnings will need time to consider, plan, and act after they receive a warning message. This is particularly true among individuals with disabilities and people with access and functional needs. They may require additional time to evacuate or may be at increased risk of harm without notification.
- Use of large-scale, wide ranging public warning systems are usually restricted to designated officials (Alerting Authorities). Operational Areas should ensure all local jurisdictions (cities, special districts and, when appropriate, private sector critical infrastructure) have the capability and a method to request the coordination and use of large-scale, wide ranging public warning systems when appropriate. When imminent danger threatens, all agencies can, and should, issue a warning to people with whom they have authority and responsibility to inform, using whatever means are at their agency's disposal.
- Messages should come from an authoritative source and clearly identify the originating agency. Messages originating from an anonymous or unfamiliar source will be treated with skepticism by the public. Whenever

possible, the Alerting Originator should be recognized by the target audience as knowledgeable on the threat.

- Approved Alerting Originators must only access OR-Alert through a unique, individually identified account so that every warning message is attributable to a specific individual. Use of shared "agency accounts" to control access to warning systems can undermine the enforceability of usage policies and is not allowed. All OR-Alert users should utilize a strong password for authentication. Ensuring the security of the system will reduce the chance of data breaches and ensure the public's trust in providing their contact information to an opt-in system.
- Warning messages can, and should be, updated and refined as additional information becomes available. Additionally, when the threat or warning messages are no longer applicable, a message stating it no longer applies should be sent.
- Warning messages sent in error should be updated, clarified, or retracted within ten minutes from the message being confirmed as being erroneous.

Use of Multiple Alerting Technologies and Strategy

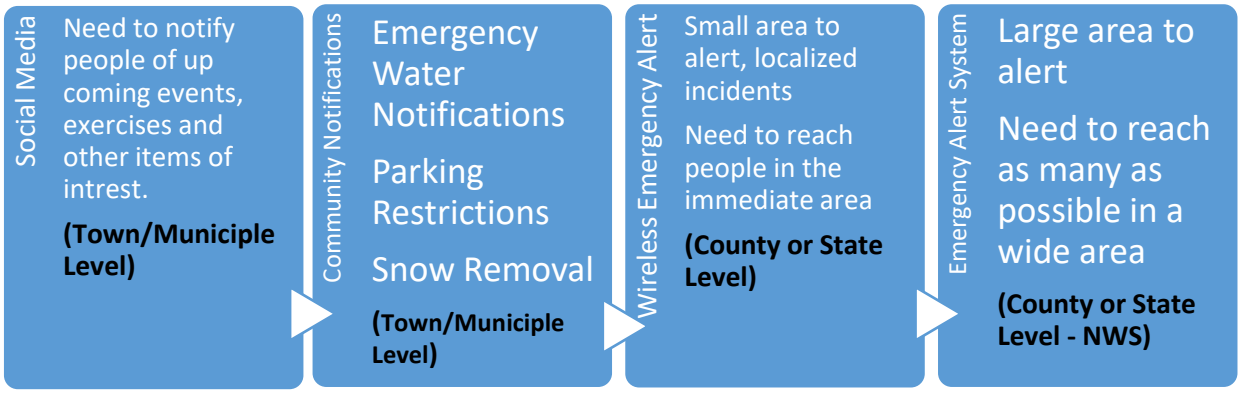
Many agencies have multiple notification/alerting systems that can be used to deliver both emergency and non-emergency information to their communities. While overlaps of tool reach may occur, each of these individual systems may also reach a distinct segment of the population in an area that other methods may not. It is therefore incumbent on the alerting authority to choose the tools necessary to reach the specific segments of the population necessary depending on the scope, and scale of event precipitating the notification. In general, the larger and more dangerous the event, the more tools will be employed. Care should be taken to not inundate the population with too many notifications, but due regard must be given to the necessity of alerting ALL people in an area affected by an emergency. This dichotomy is best addressed in advance of an emergency occurring. It is recommended that alerting authorities establish messaging strategies including thresholds, decision points, approval processes, and procedures prior to an event occurring. These strategies should be well informed by emergency communications center personnel, emergency managers, public safety leaders, members of the community, and telecommunications providers in an area. By setting an inclusive strategy well in advance, publicizing it, training, and exercising it, and employing it during an incident, jurisdictions are much more likely to strike a balance between over alerting and getting the message to those who need it that jurisdictions who do not prepare for such an event.

In all cases, careful consideration should be taken to ensure that non-emergency information is **NOT** sent via IPAWS, including WEA and EAS. [2]

[2] See Section 8: System Use Not Permitted

Jurisdictions may find the chart below helpful when deciding what methods to use to disseminate information.

Methods of Dissemination



Section 5: Training and Testing

Training

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.

The OR-Alert program supports the below role-based training resources based on the current vendor, Everbridge. Also supported are FEMA web based IPAWS training courses:

Any member of a PAA agency whose duties include disseminating public alerts, warnings and notifications must complete all required FEMA Independent Studies course(s) at the time of application or renewal. Each PAA is responsible for ensuring and documenting that their designated users are properly trained, and all certifications are current.

Recommended Role-Based Training

	EB: Account Admin Curriculum	EB: IC Admin Certificate	EB: IC Operator Certification	EB: Group Mngr Curriculum	EB: MN Msg Sender Certification	EB: Intro to Contact mngmt	EB: Managing and maintaing Contact Data	EB: How to upload Contacts	EB:How to Back-Up Contacts and User Data	EB:Contact Upload Options	FEMA-:IS-247 IPAWS Training	EB: IPAWS Admin Training	EB: IPAWS Sender traning
Account Admin	X										X	X	
Org Admin	X										X	X	
Ic Admin		X									X	X	
IC Operator			X								X		X
Group Mngr				X									
Dispatcher					X						X		X
Data Mngr						X	X	X	X	X			
MN Operator					X						X		X
Custom Role	To be determined based on role permissions and intent of role.												

System administrators are encouraged to develop custom training curriculums based on custom roles created. Additional training can be found through current vendor resources. Recommended and optional Everbridge training for all standard roles are as follow.

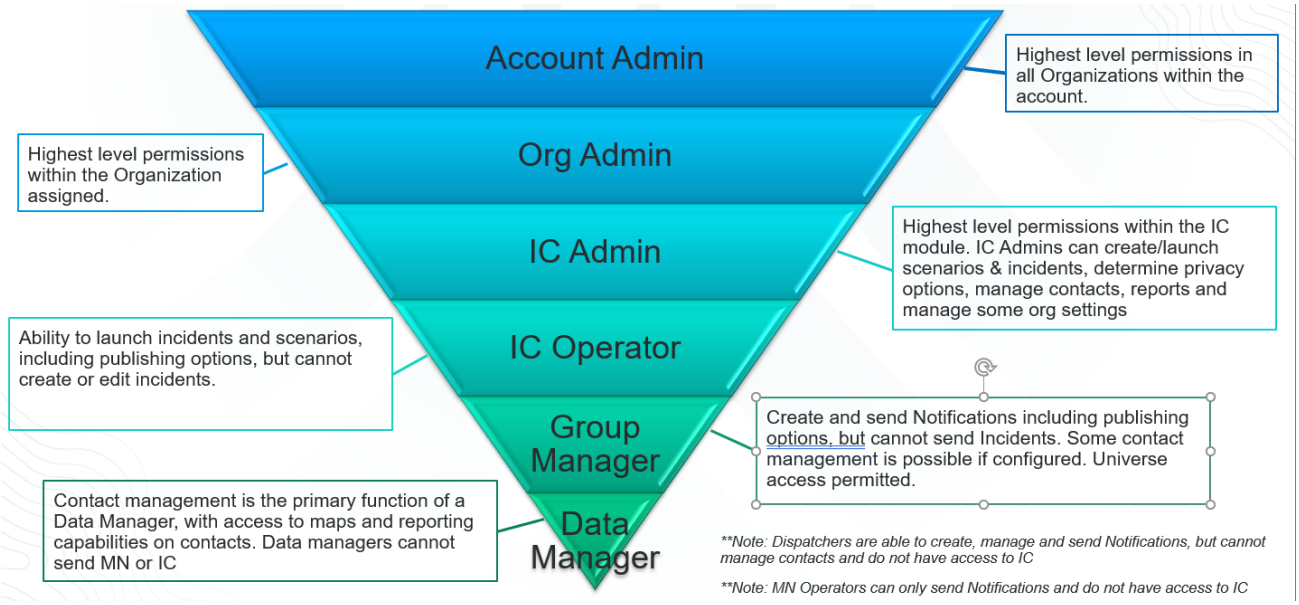
Recommended Courses for All Roles:

- Best Practices for IPAWS Messaging
- Best Practices for Smart Weather
- Nixle Best practices
- Opt-In Engagement and Event Subscriptions
- Individual evaluation and/or training with OR-Alert dedicated Technical Account Manager

An in-depth explanation of standard and configurable Everbridge Roles and permissions can be found at manager.everbridge.net under the *Access tab >Roles >Permissions Grid.*

An overview of Role capabilities is outlined below.

Overview of Roles



Training for Non-Everbridge User Jurisdictions

Jurisdictions with other system vendors may contact the OR-Alert program for recommendations on other vendor specific or vendor agnostic training recommendations. It is recommended that all alerting jurisdictions complete the FEMA IPAWS Independent Study courses through FEMA's Emergency Management Institute (EMI).

OR-Alert Testing

Required Monthly EAS Tests (RMTs)

These tests are currently done by OEM through Oregon's Primary Entry Point (PEP) Station: KOPB. Jurisdictions with analog EAS encoders are also required to test with a PEP station on a weekly basis. Tests times are coordinated with the PEP stations. These tests go to and are forwarded through broadcasters ENDEC machines and appear on television and radio.

Required IPAWS WEA Testing

In accordance with FEMA guidance, all PAAs will be required to perform a monthly test alert to the IPAWS Message Viewer testing platform. PAAs can perform this test by using an issued COG test ID issued by FEMA. This will allow

PAAs to send an actual WEA message, with real alerting codes, in a safe testing environment.

Extensive documentation[3] is available from the State IPAWS Administrator to include:

- *IPAWS Message Viewer Instructions v4*[4]
- *Testing with the IPAWS Lab Checklist*[5]
- *State EAS Plan*[6]

Please note:

- 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 their state IPAWS Reviewing Authority 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.

PAA Jurisdiction Testing and Training Plans

In addition to the required IPAWS testing, each PAA Jurisdiction should have a monthly testing and training plan to ensure operational readiness. Jurisdictions should plan and conduct assessments of every component of their alert and warning program and identify the appropriate testing cycles for each piece. Systems that are used frequently (at least monthly) may not require system testing frequencies as aggressive as those that are used less frequently.

PAAs are required to conduct regular training and exercises, including tests, of all components of their OR-Alert system to ensure the ability to send emergency notification information across the entire program. Any impediments should be identified, and a resolution developed.

It is also important to understand testing limitations. For example, it is not allowable to test on unlisted or 9-1-1-database phone numbers. Users should instead test these systems utilizing agency owned numbers.

[3] Vendor specific IPAWS procedures are available on Basecamp or through the Statewide Interoperability Program.
[4] This document can be found at https://www.fema.gov/informational-materials
[5] This document can also be found at https://www.fema.gov/informational-materials
[6] This document may be found at https://www.fcc.gov/file/13253/download

The OR-Alert program can provide technical assistance in developing training plans and exercise injects related to alerts and warnings. Jurisdictions should send a request to OR.Alert@das.oregon.gov for assistance.

Section 6: Establishing Internal Polices and Operating Procedures

The OR-Alert Program requires establishing SOPs for alerting that comply with rules of behavior and a jurisdiction's alerting objectives. SOPs should address:

- Types of alerts that will be issued
- Alerting roles, responsibilities, and authorities
- Criteria for issuing an alert, including establishment of trigger points for alerting based on specific hazards a jurisdiction is likely to face
- Message drafting and approval process
- Message dissemination strategy
- Training of staff
- Identification of back up alert originators both inside and outside of the jurisdiction who have access to the system and can originate alerts if primary is not available
- Coordination with other agencies
- Security procedures
- Testing of the system
- Cancellation or correction procedures
- Procedural checklists
- Neighboring jurisdiction coordination plan
- Public education strategy on jurisdiction's alerting plan.

Alert Activation Planning

Each PAA should identify a plan for issuing alerts in their jurisdiction/area of responsibility and establish an alternate plan for issuing alerts and warnings should the primary method become inoperable or unavailable. For example, in one jurisdiction, the county emergency management office may be the primary alert originator, while the Emergency Communications Center (PSAP) is the alternate.

If primary and alternate methods are unavailable, OR-Alert Everbridge users may initiate a message by contacting the Everbridge Emergency Live Operator Service at 877-220-4911. Users should be prepared to provide their username and answer their security question.[7]

[7] Live operators may only send messages utilizing the permissions level of the user calling in. If a higher level is needed, contact the OERS 24 hour Operations center at (800) 452-0311.

Alternatively, if a jurisdiction can no longer issue a message via their primary or alternate methods, then OEM will serve as the back-up (emergency) alerting agency. It is the responsibility of the PAA to notify the OEM Executive Duty Officer (EDO) through the Oregon Emergency Response System (OERS) 24Hr Operations Center at (800) 452-0311 immediately upon realization that the PAA alerting capabilities are unavailable.

Everbridge Emergency Live Operator Service:
1-877-220-4911

Oregon Emergency Response System
1-800-425-0311

IPAWS Approved Codes

The State IPAWS administrator, OEM, establishes what alerting codes authorities are authorized to use within Oregon. All codes are authorized for WEA except BLU (Blue Alerts). The use of CAE (Child Abduction Emergency) is restricted to the Oregon State Police. EAS codes are approved by the State Emergency Communications Committee (SECC) as outlined in the Oregon EAS Plan. Based upon the approved codes, local jurisdictions should plan when they will send each type of message and under what circumstances, who will be responsible, and what systems will be used.

Table 1: Approved IPAWS Codes

Event Code	Event Description	WEA	EAS	NWS
ADR	Administrative Message		X	
AVA	Avalanche Watch			X
AVW	Avalanche Warning	X		X
BLU	Blue Alert	NOT AUTHORIZED		
CAE	Child Abduction Emergency	OSP ONLY		
VDW	Civil Danger Warnings	X		X
CEM	Civil Emergency Message	X	X	X

DMO	Practice/Demo Warning	X		
EQW	Earthquake Warning	X		X
EVI	Evacuation Immediate	X	X	X
FRW	Fire Warning	X		X
HMW	Hazardous Materials Warning	X		X
LAE	Local Area Emergency	X		X
LEW	Law Enforcement Warning	X		X
NUW	Nuclear Power Plant Warning	X		X
RHW	Radiological Hazard Warning	X		X
RMT	Required Monthly Test		X	
RWT	Required Weekly Test	X	X	
SPW	Shelter in Place Warning	X		X
TOE	9-1-1 Telephone Outage Emergency	X	X	X
VOW	Volcano Warning	X		X

Making the Decision to Issue an Emergency AWN:

Part of OR-Alert's mission is to provide "people in Oregon with meaningful opportunities to make life-saving decisions in the face of emergencies." Without such information, people are forced to make decisions without understanding potential risks or dangers, or without understanding the scope of an incident. This may lead to casualties, up to and including the death. Therefore, it is vital that all jurisdictions take responsibility for providing vital information to the public as soon as possible during an emergency.

Emergency AWNs must be issued when there is an imminent threat to life, health, or property. This can include alerts and warnings issued in advance of forecasted severe weather events when doing so will give the public time to evacuate. When a threat exists that might not be imminent, such as a Red Flag Warning, severe weather, or flooding, it is advised to communicate that threat out to the public. Fear of triggering "panic" is not a valid reason to delay or avoid issuing a warning. Mass panic rarely occurs as the result of a warning message.[8]

[8] Note that justified anxiety or physical flight is not the same thing as panic. When public warning information is delivered by a credible alerting authority, the public usually responds by following the recommended actions. Rarely do such warning messages lead to mistrust or panic.

When dealing with uncertain or conflicting information about a threat, the Alerting Authority should choose to err on the side of protecting the public and take action as appropriate. It is always better to send an alert when life may be in danger, than not.

To ensure life safety messages are received and acted on by the public, jurisdictions should do everything possible to avoid irrelevant warnings than can fatigue the public rapidly and lead to recipients discounting further warning messages or opting out of receiving future alerts and warnings. Every effort should be made—within the capabilities of the warning system(s)—to limit the warning to people at risk. Jurisdictions can utilize the following best practices to ensure that messages are received and acted on during an emergency:

- Identify the authoritative source sending the message.
- Ensure it is clear where the emergency is happening.
- When possible, provide maps, or other resources to help the public understand where the alert is for and who is affected.
- Utilize structured training and practice to reduce false alarms.
- Immediately cancel, update, or revise messages sent erroneously or that contain incorrect information.

While repeated false alarms can damage the credibility of both the source and the delivery channel, false alarms or erroneously issued warnings historically have not significantly eroded public confidence in issued warnings as long as they were promptly corrected or retracted.[9] Warning originators should use their best judgment but err on the side of public safety.

Agencies should issue alert and warning messages as soon as feasible given the circumstances of the situation. Designated alerting staff should have ready and reasonable access to primary or back-up alerting systems and be properly trained and well versed in how to operate the equipment.

Criteria and Considerations for Issuing Emergency Messages

When circumstances arise and the need for a public warning becomes necessary, the decision to send a message will ultimately be a matter of local judgment. To assist in the decision-making process the following criteria may be applied:

- What is the size of the event? Widespread or localized?
- Does the hazardous situation require the public to take immediate action?
- Does the hazardous situation pose a serious threat to life or property?
- Is there a high degree of probability the hazardous situation will occur or escalate?

[9] See Section 10: Erroneous or False Alert Procedures

- Are there protective actions the public can take to mitigate the effects of the incident? How much time is needed?
- Is the risk widespread or does it only affect a certain segment of the population (ex: unsheltered vs. sheltered)?
    - Will the alerting tools available reach the affected population?
- Will the alert potentially harm the public or hamper response efforts? (Ex: Capacity of evacuation routes, impact on 9-1-1, alerting an active shooter to a recipient's location)

If the decision is made to issue an alert, the following should be included in the message: Please note that based on IPAWS version status, the alerting authority may be limited to 90 characters for WEA messages but should also include a 360-character message whenever possible.

Source:

- Who is issuing the warning?

Hazard:

- What is/are the hazards that are threatening?
- What are the potential risks?
- When should people act?

Location:

- Where will the impacts occur?
- Is the location described so those without local knowledge will understand their risk? (Use known streets, landmarks, terms, etc. do not use coordinates).

Guidance:

- Protective Actions: What protective measures should people take and when?
- If evacuation is called for, where should people go and what should they take with them.
- How long will the impact last?

Time / termination:

- Expiration of warning

Section 7: Equitable, Accessible, Culturally and Linguistically Appropriate Messaging Considerations

Delivery of Messages to Populations with Access and Functional Needs

Emergency alerts and warnings should account for the wide array of communication needs found in the public. When providing emergency alerts and notifications, it is vital for local, state, and federal governments understand that not everyone accesses, receives, processes, or acts upon information in the same manner. To plan effectively for these differences, emergency managers must apply a whole community approach to how they alert during an emergency or incident.

Alerting authorities should seek information and planning resources from agencies experienced with these matters such as US Department of Justice, FEMA, the US Department of Human Services (HHS), Centers for Disease Control and Prevention (CDC), Pacific ADA or other like agencies to explore ways to better meet the needs of those with access and functional needs.

OR-Alert Templates

To support language access in Oregon, OR-Alert statewide templates will be evaluated for inclusivity, diversity, equitability, and accessibility by subject matter experts and community-based organizations that might be representative of access and functional needs communities will be given the opportunity to provide comment and input. Templates will be translated into Spanish at a minimum.

Section 8: System Use Not Permitted

Non-emergency Information Usage

Non-emergency use generally refers to community outreach and public information dissemination.

While permitted, non-emergency notifications should be used carefully, with the understanding that numerous messages will dilute the effectiveness of emergency notifications and can erode confidence in the system.

Non-emergency notifications may be transmitted utilizing Opt–in methods within the MNS (i.e., Nixle keywords, community engagement, public member portals, etc.), with the approval of the system administrator or in compliance with local policies. All non-emergency notifications must be compliant with all laws, local ordinances, regulations, rules, and with the requirements of the Oregon Ethics Commission.

Non-Emergency messages may not be sent via:

- IPAWS (testing excepted)
- Enhanced telephone notification (i.e., Resident Connect, Reverse 9-1-1, or other systems utilizing public databases)

Prohibited non-emergency notifications include:

- Any message of a commercial nature
- Any message of a political nature
- Any non-official business
- The use of any individual’s name not related to a public safety condition or event

Section 9: Cross-Border / Neighboring Jurisdiction Notification and Coordination

Alerting Coordination

Disasters are not typically limited to jurisdictional boundaries; however, Alerting Authorities are generally bound to their own jurisdiction. When considering issuing an alert and/or warning to the public, jurisdictional coordination, communication, and collaboration should be a priority.

To the extent a warning originator has the ability, warnings should be targeted to the area known to be at risk, while coordinating with any other affected jurisdictions as soon as possible. If the initial warning originator lacks the ability to deliver warnings to the at-risk area, coordination with other jurisdictions should be given priority.

If a warning is issued from a higher level of government or jurisdiction, lower levels within the target area of the initial warning need not repeat that warning. However, local jurisdictions should issue additional warning messages, or request assistance from an Alerting Authority, if needed, to communicate local variations on the recommended protective action, to expand the target area for the message, or to utilize local warning dissemination capabilities that will enhance delivery of the warning to people at risk.

Evacuation messages are particularly demanding on their originators, as they must be coordinated with agencies responsible for transport, traffic control, and evacuee reception and sheltering. Confusing and/or uncoordinated evacuation orders can have unintended adverse consequences. Evacuation messages must come from the jurisdiction's designated authority, often the local law enforcement authority and within the capabilities of the technologies available could address issues such as:

- Travel Information (recommended route, means of travel, direction).
- Accessible transportation and sheltering resources.
- Phone, social media, or weblink for additional information.

Cross-jurisdictional Alerting

It is strongly recommended that cross-jurisdictional alerting be accomplished through a formal agreement process that addresses:

- When and under what conditions cross jurisdictional alerting may occur.
- Roles and responsibilities of partner agencies.
- Establishment of agreed upon alerting criteria.
- Establishment of procedures for cross jurisdictional alerting.
- Defining how cross jurisdiction alerting will occur and how any technical obstacles will be overcome. (Ex: permissions within the system, shared

IPAWS Specific Area Message Encoding (SAME) codes, and/or other methods).

- Establishment of minimum required training.
- Any necessary privacy, security, legal concerns.

The OR-Alert Program encourages jurisdictions to work together whenever possible to ensure that all members of the community and those that may be traveling through an area are alerted during an emergency. The Program can assist jurisdictions with developing shared policies, procedures, and agreements to accomplish cross-jurisdictional alerting. Requests for assistance may be sent to OR.Alert@das.oregon.gov.

Section 10: Erroneous or False Alert Procedures

Structured training and practice will reduce false alarms. While repeated false alerts can be damaging to the credibility of both the source and the delivery channel, false alerts or erroneously issued warnings historically have not significantly eroded public confidence in issued warnings as long as they were promptly corrected or retracted.

If an erroneous, false, or misleading message is sent, the public in the alerted area should be notified immediately via the same means that the original alert was sent out.

PAAs should have procedures in place for such an event. In the case of an erroneous alert or warning, it is recommended that the issuing agency head, and PIO staff be immediately notified.

It is also recommended that the OEM EDO be notified through OERS for situational awareness. OERS may be contacted at 1-800-425-0311.

If a false WEA or EAS message was sent, then it is required that the FCC 24 Hour Center be notified within 24 hours of such message being sent. The notification can be sent to the FCC Public Safety and Homeland Security Bureau (PSHSB) 24/7 Operations Center via the email or telephone number listed below:

FCCOPCenter@fcc.gov
(202) 418-1122

Section 11: System Management

The following section is specific to the current OR-Alert Vendor: Everbridge.

System settings are designed to streamline outgoing alerts, warnings, and notifications so that messages reach recipients faster and through more modalities, while mitigating confusion.

The following are recommendations and best practices as they relate to key Everbridge Suite system settings.

Template Settings

- Customize Message Templates per Delivery Method: Compose separate messages based on individual delivery methods, expectations associated with each delivery method (e.g., length), and technical limitations of delivery method (e.g., GSM characters and character count).
- Delivery Methods: Preconfigured to accommodate a variety of modalities such as voice call (using a voice recording), SMS, webpage, email, fax, pager, Everbridge mobile app and TTY.
- Publishing Options: Preconfigured to include EB Network- State of Oregon private group, Premium Audio Bulletin Board, Member Portal, social media and Nixle channels.
- Incident Zone: Enabled when using a geographic boundary to notify impacted recipients.
- Confirmation: Set to “yes” (This is the best way to avoid recipient fatigue, by offering them the means to confirm and stop messages while also giving message senders confirmation details).
- Delivery Order: Organizational default chosen as delivery order if sending to a large area or jurisdiction.
- Voice Mail Preference: Set to “message only”.
- Everbridge Mobile App Setting: Enable sharing options.

Map Settings:

- Map Default: Set to most active or central part of jurisdiction to mitigate map navigation time when selecting contacts.
- Shape Library: Upload commonly used shape files such as jurisdictional boundary maps, flood plains, evacuation zones, power safety power shut off zones, etc..

CAP Channel Settings

- Ensure IPAWS live and test certificates are successfully uploaded, and COG profile matches MOA and Alerting Authority.
- Update SAME codes, sender agency name, and CAP RSS defaults. Defaults can be changed at time of sending IPAWS message but should be set for most common IPAWS alerts.
    - Category: Safety

- Scope: Public
- Urgency: Immediate
- Severity: Extreme
- Certainty: Observed

Notification Settings

- Default options, General:
  - Imminent Threat to Life: Set to on. (This provides the option to send a message as imminent threat to life if need be).
  - Request Confirmation: Set to on (This allows recipients to confirm and stop messages to avoid recipient fatigue).
  - Interval Between Delivery Methods: Set to 2 minutes; in the event of an urgent emergency the sender may opt to change interval to 1 minute or zero minutes for faster delivery, but 2 minutes will give recipients a chance to confirm and stop the message before becoming fatigued.
  - Voicemail preference: Set to “message only”.
- Default Options Incidents:
  - Scenario Manager; Set to on.
  - Exercise Mode: Set to on.
  - Incident Notification Review Step: Set to on (Required is optional).
- Short Message Service (SMS)
  - Including the title in SMS is optional, but because it counts against SMS character count it is not commonly utilized.
  - Header on SMS URL Web Page: Enter agency name, this will become the header on all webpage SMS messages for added authentication and branding.
  - Custom badge: Upload image file for added authentication; agency logo will be displayed next to SMS Header.
- Delivery Methods:
  - Order delivery methods so that landline codes are last in delivery order to mitigate slowing of message delivery if physical infrastructure is overwhelmed. It is recommended the EB Mobile app is 1st, email 2nd (email typically provides the most comprehensive information to reference), SMS 3rd.
  - Allow Unsubscribe From: Phone = No, Email = No; This will only unsubscribe the recipient from this delivery method and not all other methods. It is best to direct recipients to the member portal to unsubscribe.
  - Broadcast Throttling Rules: Set to carrier recommendations.
  - Phone Voice Greeting: A custom non-priority and priority greeting is recorded. A human voice is more trusted than the computerized default message and may mitigate recipients hanging up before hearing the message.
    - Sample Non-Priority Greeting: This is a message from OR-Alert.

        - Sample Priority Greeting: This is an emergency message from OR-Alert, please do not hang up.
    - Email Header & Footer:
        - Header: Include the agency name and logo in header for authenticity.
        - Footer: Include agency contact information or additional instructions such as “If you would like to change the way you receive messages, go to [member portal link].”
        - Optional: The member portal also provides a means for visitors to translate the portal to the language of their choice, and therefore translate notifications posted to the portal. Agencies might consider including a message in primary non-English language(s) directing people to the member portal for translation.

Member Portal Settings:

- Google Translate: Enabled.
- Locations: Geofence is enabled using a jurisdictional boundary shape file (including or excluding a buffer).
- Smart Weather Alert Subscriptions: Active and includes member modification of quiet periods with severe weather events checked as a quiet period override.
- Delivery Methods: All exposed delivery methods are editable and at least one non-specific contact path is required.
- Content: Banner uploaded including agency name, logo and powered by OR-Alert logo[10].
- Log In Pages: Contains clear expectations for what visitors can expect when registering for agency alerts. May also include additional instructions to aid visitors in navigating site, such as “sign in” vs “sign up” instructions or who to call for assistance.
- Informational Pages: Customize overview and FAQ pages to accommodate your jurisdiction.

Mobile App:

- Enable Organization Search: Enter full agency and/or alerting name (or both) as organization display name.
- Require Exact Match: Deselect.
- Search Terms: In a single cell, enter all possible search names associated with your jurisdiction such as abbreviations, nicknames, major city names and zip codes. Ensure all terms are comma delineated and within a single search cell.

[10] See Appendix F

Section 12: System Security

Every system user is responsible for access security as it relates to their use of OR-Alert and shall abide by these Rules of Behavior:

- All users must have a discrete user account ID which cannot be the user's social security number. To protect against unauthorized access, passwords linked to the user ID are used to identify and authenticate authorized users.
- Accounts and passwords shall not be transferred or shared. The sharing of both a user ID and associated password with anyone (including administrators) is prohibited.
- Agencies are required to revoke access for those who no longer require access to the system. Agencies shall immediately revoke access to the system for any user who involuntarily separates from employment with the Agency. Agencies shall revoke access to the system for any user who voluntarily separates from employment or affiliation with the Agency within 24 hours.
- Agencies shall only permit authorized users to access the system via Agency-owned electronic devices unless such limitation would prevent the sending of a message in an imminent or life-threatening emergency.
- Accounts and passwords shall be protected from disclosure and writing passwords down or electronically storing them on a medium that is accessible by others is prohibited.
- Passwords must not contain names, repetitive patterns, dictionary words, product names, personal identifying information (e.g., birthdates, social security numbers, phone number), and must not be the same as the user ID.
- Passwords must be greater than eight (8) numbers, letters or characters with at least one item from three of the following four criteria: an uppercase letter (A-Z), a lowercase letter (a-z), numerals (0-9), and/or special characters: !, @,#,$,%,^.&.*,(,). Additionally, passwords must and follow the Oregon Department of Administrative Services Information Technology (DAS IT) accepted guidelines. Recommended best practices are noted below, per the Oregon Statewide Information and Cyber Security Standards:

  Password Construction:

  - Minimum length of ten (10) characters.
  - At least one (1) numeric (e.g., zero – 9) and one (1) non-alphanumeric character (e.g., @, #, $, %, ^, &, etc.).
  - At least one (1) English uppercase letter (e.g., A – Z).
  - At least one (1) English lowercase letter (e.g., a – z).
  - No dictionary words or common names.

- No portions of the associated account name / identifier (e.g., User I.D., login name).

Password Administration:

- Minimum lifetime of one (1) day.
- Maximum lifetime of 90 days.
- Change a password immediately in the event of a suspected compromise of the password or system.
- The current OR-Alert vendor does not allow re-use of the last three passwords. It is recommended, through policy, to prohibit use of the last 24 passwords.

- Passwords must be promptly changed whenever the compromise of a password is known or suspected.
- Users accessing IPAWS: Physically protect computing devices such as laptops, computer gaming consoles, smartphones etc.; protect sensitive data sent to or received from IPAWS; do not program computing devices with automatic sign-on sequences, passwords or access credentials when using IPAWS.
- Users will not provide or knowingly allow other individuals to use their account credentials to access IPAWS.
- To prevent and deter others from gaining unauthorized access to sensitive resources, users will log off or lock their computer workstation or will use a password-protected screensaver, whenever user steps away from a workstation area, even for a short time and will log off when leaving for the day.
- Inform the local system administrator when access to IPAWS is no longer required.
- Promptly report security incidents to the Local System Administrator and the State IPAWS Coordinator.
- All employees should receive cybersecurity awareness training and should follow cybersecurity best practices in protecting both IPAWS physical access equipment and network access.
- Only trained and certified users should be allowed access to the IPAWS software.

Section 13: Records and System Currency

The OR-Alert Program is the records custodian for records related to the OR-Alert Governance Committee, the system contract, Interagency/Inter-Governmental Agreements, and records related to program administration.

Individual agencies, counties, tribes, localities, and organizations are responsible for their individual records related to the system and the issuance of alerts, warnings, and notifications. The system automatically purges records and reports at certain intervals. Participating entities are advised that they are solely responsible for downloading needed records and/or reports prior to the automated purge date.

The following section is specific to the current OR-Alert vendor: Everbridge

Everbridge will retain historical Notifications and Incidents for 18 months. System Administrators should assign records to be exported and archived prior to 18 months. Records will not be accessible, even by Everbridge, post 18 months.

Everbridge will retain deleted contacts for 30 days after they are deleted, after which, contacts cannot be restored.

Keeping contact data current is vital to effective messaging. Many agencies will campaign annually or bi-annually to encourage community members to revalidate subscriber contact information and alerting preferences through their member portal. New subscribers are also encouraged to register for alerts. Additionally, users may regularly run reports to identify “bad” or incomplete contact data and make effort to resolve prior to an emergency alert.

Internal contact data such as employee’s, vendor’s, and contractor’s information are also vital in keeping internal partners informed. Utilizing a private member portal, and/or setting up contact data to be automatically updated on a reoccurring schedule is recommended.

Finally, ensuring groups and rules are also current will enable message senders to target the right people successfully and efficiently at the right time.

Users and permissions should be reviewed on a regular schedule. If an agency has high turnover, a monthly review may be beneficial. For smaller or less active agencies, an annual review may be appropriate. It is important to ensure users have access to necessary functions, templates and contacts, and that redundancies are built in to accommodate for absences and other unavailability. User permissions should be suspended, or users deleted, once terminated or when they no longer should have access to the system.

Appendix A: IPAWS Application Process

The State IPAWS Administrator has the authority to approve applications for IPAWS Alerting Authorities within the state. It is recommended that agencies desiring to obtain alerting authority contact the State IPAWS Administrator prior to purchasing any software or equipment. It is the IPAWS Administrator's responsibility to ensure that adequate and proper alerting responsibilities are assigned. Copies of all documents referenced below are available from the State IPAWS Administrator.

How to apply for IPAWS:

1. Contact the State IPAWS Administrator for prior approval and guidance.
2. Select an IPAWS compatible software. Access to IPAWS is free; however, to send a message using IPAWS, an organization must procure its own IPAWS compatible software. A list of private sector developers can be found at https://www.fema.gov/media-library/assets/documents/25916.
3. Apply for a Memorandum of Agreement (MOA) with FEMA https://www.fema.gov/media-library/assets/documents/112266

   To become a COG, a MOA governing system security must be executed between the sponsoring organization and FEMA. Each MOA is specifically tailored to the sponsoring organization and their interoperable software system.

   The MOA will be sent as part of the FEMA applications process. The FEMA COG coordinator will prepare and return the MOA for signature after it is submitted and assign a COG identification (ID). After being signed by the applicant, the MOA will be routed for FEMA signatures. A copy of the executed MOA and the COG-specific digital certificate will be returned to the sponsoring organization. Both the COG ID and digital certificate are necessary to configure the IPAWS compatible software system.
4. Apply for public alerting permissions

   You will receive a public alerting application along with your unsigned MOA. This application must be signed by the designated state official. The State IPAWS Administrator.

   - Complete this application defining the types of alerts a COG intends to issue and the extent of its geographic warning area. The contact information for the designated state reviewer will be provided with the public alerting application.
   - This form will be submitted for approval to:
     - The Oregon Department of Emergency Management attention Doug Jimenez: doug.jimenez@oem.oregon.gov

- Once the signed form is received, please send it to IPAWS@FEMA.DHS.GOV .

5. Complete IPAWS web-based training
   - Complete IS-247.A http://training.fema.gov/EMIWeb/IS/is247a.asp
   - Send the Certificate of Achievement to:
     - Oregon Department of Emergency Management attention Doug Jimenez: doug.jimenez@oem.oregon.gov
     - FEMA at: IPAWS@FEMA.DHS.GOV

THIS SPACE INTENTIONALLY LEFT BLANK

Appendix B: Acronyms

Acronym	Description
AAR	After Action Review
AMBER	America's Missing Broadcast Emergency Responder
AWNs	Alerts, Warnings and Notifications
CAE	Child Abduction Emergency
CDC	Centers for Disease Control and Prevention
CMSP	Commercial Mobile Service Provider
COG	Collaborative Operating Group
DAS IT	Department of Administrative Services Information Technology
EAS	Emergency Alert System
EDO	Executive Duty Officer
EMWIN	Emergency Managers Weather Information Network
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing System
FNF	Fixed Nuclear Facility
HAZMAT	Hazardous Materials
HHS	Health and Human Services
ID	Identification
IPAWS	Integrated Public Alert and Warning System
IS	Independent Study (FEMA online training)
MOA	Memorandum of Agreement
NCC	Oregon State Police Northern Command Center
NOAA	National Oceanic and Atmospheric Administration
NWEM	Non-Weather Emergency Messaging
NWS	National Weather Service
NWWS	NOAA Weather Wire Servce
OAB	Oregon Association of Broadcasters
ODOT	Oregon Department of Transportation
OEM	Oregon Department of Emergency Management
OERS	Oregon Emergency Response System
OSP	Oregon State Police
PAA	Public Alerting Authority

PIO	Public Information Officer
POTUS	President of the United States
PSAP	Public Safety Answering Point
PSHSB	FCC Public Safety and Homeland Security Bureau
PUC	Public Utility Commission
RMT	Required Monthly Test
RWT	Required Weekly Test
SAME	Specific Area Message Encoding
SECC	State Emergency Communications Committee
SCRAP	Sub-Committee for Recommendations on Alerting Practices
SIEC	Statewide Interoperability Executive Committee
SMPP	Short Message Peer-to-Peer
SMS	Short Message Service
SOP	Standard Operating Procedures
SWIC	Statewide Interoperability Coordinator
SWIP	Statewide Interoperability Program
TDD	Telecommunications Device for the Deaf
TTY	Teletypewriter
WEA	Wireless Emergency Alerts

Appendix C: Template WEA policy

Irrelevant warnings can fatigue the public rapidly and lead to recipients discounting further warning messages or opting out of receiving future alerts and warnings. Every effort should be made, within the capabilities of the warning system(s), to limit the warning to people who are at risk. Warning systems become more effective to the extent they can target limited areas or specific at-risk populations.

Public Alert and Warning

Wireless Emergency Alerts (WEA)

Created:	**Author:**	**Approved:**

System Use

Authorized Use

- Activation of Wireless Emergency Alerts (WEA) through the Integrated Public Alerts and Warning System (IPAWS).
- A localized (local public alerting authority) short duration emergency incident that threatens lives, for which the public needs to take protective action(s) (Evacuate, shelter-in-place, etc.).

Prohibited Use

- AMBER Alert messages must originate from a law enforcement to OSP for broadcast.
- Weather-related messages are originated by the National Weather Service (NWS).
- Non-emergency information shall not be sent over IPAWs.

Directives

- All local WEA messages will be coordinated through *(Name)* County Emergency Management.
- Local Emergency Management will coordinate activation of IPAWS for qualifying incidents on behalf of public safety agencies with jurisdiction in *(Name)* County.
- Local Emergency Management will coordinate with ancillary public alerting authorities (PAA) in applicable areas (Military Bases, Universities, etc.)
- Local Emergency Management will consider the following general guidelines for qualifying local activations of WEA:
  - Severity of situation – WEA warning will aid in reducing loss of life or substantial loss of property.
  - Timeliness – Immediate public knowledge is required to avoid adverse impact.
  - Alternatives – Other means of disseminating information are inadequate to ensure rapid delivery.

Initial Focus & Recommended Actions

Task #	Completed	Description
1		Determine from the agency requesting a WEA message: • **Source:** *Who is issuing the warning* • **Hazard Characteristics:** *Information on the impending hazard* • **Location:** *Specific information regarding a geographic location* • **Consequences:** *What will happen to people if they do not act* • **Protective Action:** *What people need to do to get away from the danger* • **Protective Action Time**: *How much time people have to accomplish protective action(s)* • **How action reduces consequences:** *Acting will result in the following safety consequence* • **Expiration Time:** *When this message expires or is no longer valid*
2		Responsible entity will prepare and send message in accordance with the above information. The message must be less than 360 characters.

3		Optional: Contact the Oregon OEM Executive Duty Officer by requesting they be paged through the Oregon Emergency Response System at 1-800-425-0311 and advise them that a WEA message was sent. Email OEM_OEMEDO@oem.oregon.gov a completed copy of the WEA message to the OEM 24-hour Communications Center.
4		If applicable, contact the National Weather Service to request activation of the NOAA weather radios.
5		WEA message should be followed up with general public information issued through agency public information officers (PIO) to include: • Social media releases • Local media involvement (television, radio, etc.)
6		If applicable, a follow-up message should be sent to update the situation or terminate an emergency.

Hazards and Corresponding Public Alerting Method

Hazard	Event Code	Authorized By	Local Alerting (Opt-in)	IPAWS/WEA
Avalanche Warning	**AVW**	**National Weather Service**	**Yes**	**Yes**
Blue Alert	**BLU**	**Local Municipalities, Emergency Management**	**Yes**	**Yes**
Civil Unrest/Civil Danger	**CDW**	**Law Enforcement, Emergency Management**	**Yes**	**Yes**
Civil Emergency Message	**CEM**	**On Scene Incident Command (IC), Local Municipalities, Emergency Management**	**Yes**	**Yes**
Practice/Demo Warning	**DMO**	**Emergency Management, Public Alerting Authority**	**Yes**	**Yes**
Earthquake (post incident)	**EQW**	**Local Municipalities, Emergency Management**	**Yes**	**Yes**
Evacuation Immediate	**EVI**	**On Scene Incident Command (IC), Local Municipalities, Emergency Management**	**Yes**	**Yes**
Fire Warning	**FRW**	**On Scene Incident Command (IC), Local Municipalities, Emergency Management**	**Yes**	**Yes**
Hazardous Materials Warning	**HMW**	**On Scene Incident Command (IC), Local Municipalities, Emergency Management**	**Yes**	**Yes**
Local Area Emergency	**LAE**	**On Scene Incident Command (IC), Local Municipalities, Emergency Management**	**Yes**	**Yes**
Law Enforcement Warning	**LEW**	**On Scene Incident Command (IC), Local Municipalities, Emergency Management**	**Yes**	**Yes**
Nuclear Power Plant Warning	**NUW**	**Local Municipalities, Emergency Management**	**Yes**	**Yes**
Radiological Hazard Warning	**RHW**	**Local Municipalities, Emergency Management**	**Yes**	**Yes**

Shelter in Place Warning	**SPW**	**On Scene Incident Command (IC), Local Municipalities, Emergency Management**	**Yes**	**Yes**
9-1-1 Telephone Outage Emergency	**TOE**	**Local Municipalities, Emergency Management**	**Yes**	**Yes**
Severe Weather (Flooding, Tornado, Avalanche, etc.)		**National Weather Service**	**No**	**No**

Example Message:
"(Blank) County Emergency Management. Chlorine gas release at 700 Sandridge Rd (city/town). Toxic Cloud moving toward Madison Park. Breathing this gas will result in immediate death. Close doors and windows and turn of Air Conditioning. Drivers remain in vehicles. This must be completed in the next 10 minutes. This message will expire at XXXX am."

"From: (Blank) County Emergency Management. Armed suspect at 700 Sandridge Rd (city/town). Stay indoors and secure all windows and doors, report all suspicious activity to 9-1-1. Tune into local media for more information."

"From: (Blank) County Emergency Management. I-29 near mile marker 77 is currently closed due to flooding. Be patient. Do not call 9-1-1 unless you have an emergency, Keep the emergency lane open! Tune into local media for more information."

Appendix D: OR-Alert Issued Statewide Templates

Statewide templates are developed by the Sub-Committee on Recommendations for Alerting Practices (SCRAP) in effort to aid County Emergency Managers, Tribal Governments and State agencies in building a robust template library in preparation for potential emergencies and disasters.

Statewide templates can be accessed at: BaseCamp.com. Access to BaseCamp may be requested by contacting the Statewide Interoperability Coordinator (swic.or@oregon.gov) or the OR-Alert program's Technical Account Manager.

Appendix E: Determining User Roles and Permissions

Everbridge Suite is a role-based access control system, meaning permissions can be restricted and/or enhanced depending on the job function and decision-making authority of the system user. Except for the Account Admin role, multiple roles can be assigned to a single user. Some role permissions are customizable. A detailed list of role permissions and customizable options can be found within the Everbridge system, *User Role Permissions; Permission Grid 21.4.*

OR-Alert Everbridge Suite roles are as follow:

Account Admin: At the account level, an Account Administrator is the overall system administrator. The Account Administrator inherits all permissions of all user roles for all products available within the OR-Alert Everbridge Suite account. An Account Administrator can access all features available at the account level and at the organization level.

Organization Admin: Organization Administrators can access all features available to the organization (all OR-Alert Everbridge Suite and Incident Management tabs at the organization level). Organization Administrators can perform actions within their own organizations, but not other organizations. They can add groups in their individual organizations.

Incident Admin: An Incident Administrator manages incident communication for the organization. Incident Administrators can access features at the organization level under the Incidents, Dashboard, Contacts and Reports tab. Incident Administrators inherit all permissions of the Incident Operator.

Group Manager: Group Managers can manage and send notifications to predefined sets of contacts. Group Managers can access features at the organization level under the Dashboard, Universe, Notifications, Contacts and Reports tabs. Group Managers can perform actions within their own groups. A group Manager cannot edit the organization settings and cannot send incident notifications.

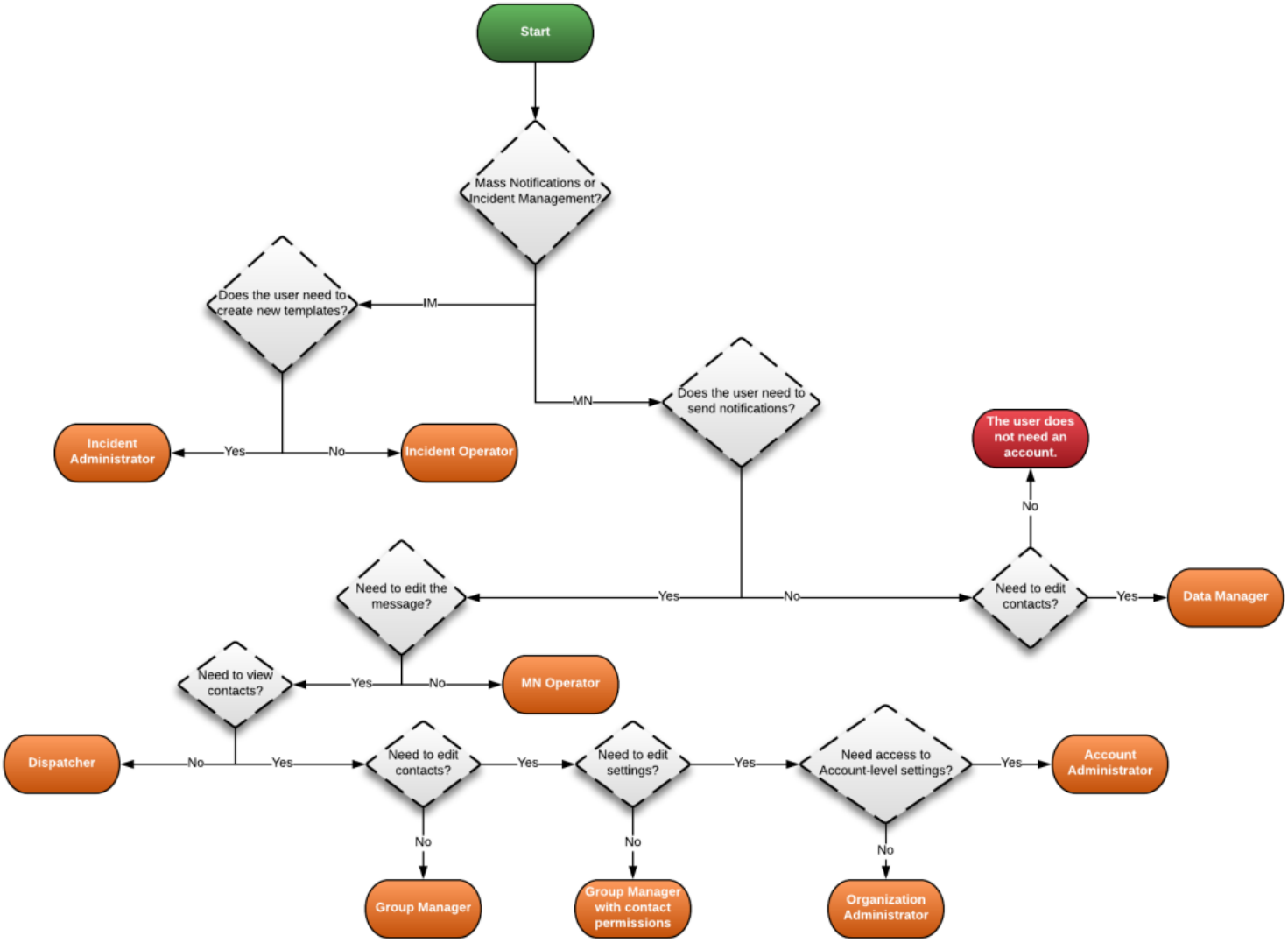
Dispatcher: Dispatchers can manage and send notification templates, manage scheduled notifications, and manage active notifications. Dispatchers can access features at the organization level under the Dashboard, Universe, and Notification tabs.

Data Manger: Data Managers can only manage contacts records (add, edit, and remove). Data managers can access features at the organization level under the Contacts and Reports tabs.

Mass Notification Operator: Mass Notification Operators can send predefined notification templates and can manage active notifications. Mass Notification Operators can access features at the organization level under the Notifications tab.

Incident Operator: Users of this role can send predefined incident templates and can manage active incidents. Incident Operators can access features at the organization level under the incidents tab.

Refer to the flow chart below to better determine the appropriate role(s) for system users.



Appendix F: - Approved OR-Alert Graphics