September 16, 2020

COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL VII

REPORT ON STANDARD OPERATING PROCEDURES FOR EMERGENCY ALERTING COMMUNICATIONS

Working Group 1: Alert Originator Standard Operating Procedures

Table of Contents

Table of Figures

Table of Tables

1 Results in Brief

1.1 Executive Summary

Standard Operating Procedures (SOPs) for communication between stakeholders (e.g., broadcasters, cable providers, wireless providers) are essential tools for both communications service providers and Alert Originators. Complete and well-developed SOPs that incorporate all stakeholders in the alert disseminations process enable faster and more effective responses during emergencies when every second may count.

This report documents the examination by CSRIC VII, Working Group 1 with respect to the following:

1) Establishing and maintaining communications between industry stakeholders (e.g., broadcasters, cable providers, wireless providers), government partners, and alert originators;
2) Developing and maintaining relationships between communications providers and alert originators that can readily be leveraged during emergencies;
3) Establishing redundant and effective lines of communication with key stakeholders during emergencies, including Government Emergency Telecommunication Service (GETS) and the Wireless Priority Service (WPS); and
4) The important elements that should be included in alert messages that retract or correct false alerts.

The first three tasks all seek to establish and maintain lines of communication among all stakeholders in the alert systems. Recommendations in this report are flexible to accommodate the different challenges that face different stakeholders, while ensuring that communications among those stakeholders is efficient and resilient and secure, supported by knowledge of not only the correct contacts and contact information, but knowledge of the responsibility and capabilities of other connected facilities and the personnel that run those facilities. This applies not only to the expected communications paths for all alerts, but also to extended paths in the case of unusual or extreme circumstances. Next steps are then offered to bring current alert status to all stakeholders in all alert facilities (Eyes on IPAWS expansion) and to guide stakeholders to continue beyond these tasks set by the FCC toward a regular exchange of information and mutual support in order to build and extend the sense of community among these people that facilitate the communication of life-saving information.

The fourth task has been addressed with specific steps and recommendations to support agency personnel with the proper training, tools and understanding of the systems to which they have access. The initial focus is on reducing the need to correct or retract false alarms by stepping up prevention of false alarms. This is followed by clear steps and considerations that should follow a false alarm.

Eight **FCC Action Items** are indicated throughout the sections containing the CSRIC VII recommendations, specifically placed in the sections that carry the related recommendations.

2 Introduction

The FCC directs CSRIC VII to recommend model emergency alerting communications SOPs that emphasize engagement with all entities that contribute to the dissemination of fast and reliable emergency information to the public.

CSRIC VII Structure

Communications Security, Reliability, and Interoperability Council (CSRIC) VII					
CSRIC Steering Committee					
Working Group 1: Alert Originator Standard Operating Procedures	Working Group 2: Managing Security Risk in the Transition to 5G	Working Group 3: Managing Security Risk in Emerging 5G Implementations	Working Group 4: 911 Security Vulnerabilities during the IP Transition	Working Group 5: Improving Broadcast Resiliency	Working Group 6: SIP Security Vulnerabilities

Table 1 - Working Group Structure

2.1 CSRIC VII Working Group 1 Team Members

Working Group 1 consists of the members listed below.

Name	Representing
Craig Fugate, WG Chair	America's Public Television Stations
Mark Annas	City of Riverside Fire Department – OEM
Terri L. Brooks (Report Editor)	T-Mobile USA
Sulayman Brown	Fairfax County, VA
Wade Buckner	International Association of Fire Chiefs
Dana M. Carey	County of Yolo, CA
Edward Czarnecki	Digital Alert Systems, Inc.
Brian K. Daly	AT&T
John Davis	T-Mobile USA (Alternate)
Ashruf El-Dinary	Xperi Corporation
John Dooley	Minnesota Department of Public Safety (Alternate)
Mike Gerber	National Weather Service (Alternate)
Matthew Gerst	CTIA-The Wireless Association®
Robert Gessner	ACA Connects
Dana Golub	Public Broadcasting Service
Mark Hess	Comcast
Antwane Johnson	FEMA
Chandra Kotaru	AWARN Alliance
Jeff Littlejohn	iHeartMedia Inc.
Michelle Mainelli-McInerney	National Weather Service
Alex McHaddad	Blue Mountain Translator District, OR
Peter Musgrove	AT&T (Alternate)
Michael Nix	Emergency Communications Authority
Donna Platt	NC Division of Services for the Deaf and Hard of Hearing
Pat Roberts	Florida Association of Broadcasters
Tim Romero	Sonoma County, CA
Craig Saari	Charter
Francisco Sanchez, Jr.	Harris County, TX
Mark Schutte	Cox
Leslie Sticht	Minnesota Department of Public Safety
John Williamson	Nez Perce Tribal Police Department
Jeff Wittek	Motorola Solutions, Inc.

Table 2 - List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objective and Scope

Alert systems in the US serve a critical function, disseminating important and sometimes life-saving information. The success of this system rests not only on the dependability of the equipment, but on how accurately and efficiently the personnel are able to perform their roles, as well as their ability to respond to, and recover from, unexpected circumstances or events. All stakeholders, including Alert Originators, government partners, broadcasters, cable providers, satellite providers, and wireless providers, must be prepared and in an always-ready state to perform their specific roles in the end-to-end process. While each task assigned to CSRIC VII explores different aspects of best practices within the stakeholders' premises, together they combine to form a complete framework to facilitate an efficient, dependable, end-to-end alert system, including recovery capabilities.

Task 1 ensures an always-ready state of communication among these essential resources. Task 1 focuses on improving communications strategies among the key industry stakeholders, government partners and Alert Originators. It looks to ensure documentation and knowledge of key contacts, backup contacts, and the procedures to exchange information.

Task 2 seeks to enhance the stability and strength of this communications structure by ensuring up-to-date knowledge of responsible parties, as well as building relationships among the leadership of the stakeholders to create mutual trust and improve responsiveness through knowledge of each other's capabilities and response style.

Task 3 addresses alternate communications strategies should the original intended system or strategies unexpectedly fail in real-time, or in the case of extreme circumstances when use of all possible avenues to speed alert dissemination is critical for public safety. Stakeholders should have both a communication and technological connection strategy to enable consistent messaging and coordination if your primary method is interrupted. It is imperative that personnel be prepared to recognize the need to include additional communication tools (e.g., GETS or WPS) into the process, and to be able to smoothly implement a switchover to, or integration of, those additional communications channels.

Task 4 targets the specific scenario of a false alert, and was included based on recent real-life events. The FCC wrote this task to ensure the establishment of clear, efficient recovery procedures to retract or correct the information already disseminated by a false alert. Due to the negative impacts to the public that will occur no matter how efficient the recovery process, we expanded this task to also address recommended practices for the prevention of false alerts.

3.2 Methodology

This report sets forth common alert recommendations, as well as some recommendations which address functionality applicable only to specific systems, such as the Emergency Alert System (EAS) and the Wireless Emergency Alert (WEA) system.

The next two sections provide an introduction to EAS and the WEA system.

3.2.1 Emergency Alert System

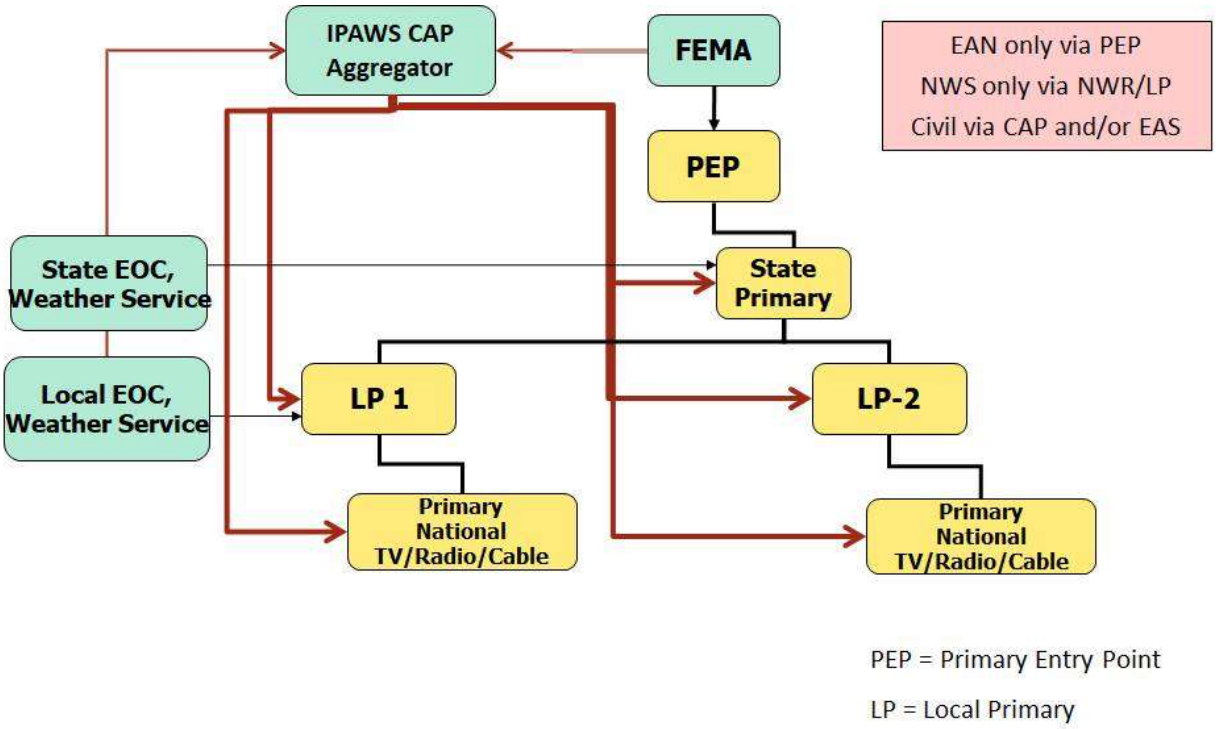

Figure 1 Emergency Alert System

The Emergency Alert System was created in the 1997, as a successor to the Emergency Broadcast System of the 1960s through 1990s, as a mechanism to pass along a Presidential Alert in the case of a national emergency. Over time, additional alerts have been added as optional alerts for more localized emergencies. These alerts were intended to be broadcast by TV and radio to the listening area.

Primary Entry Points (PEPs) are the primary source of the initial broadcast for a Presidential Alert. They are the initial receiving entity of the Presidential Alert forwarded by FEMA. Further along the communications chain, State Primaries and Local Primaries (LP-1, LP-2, etc…) may broadcast directly to the public, but are also monitored by stations not designated as PEPs, which will broadcast to the public.

The addition of video distribution by Multi-Channel Video Providers (MCVPs), including

satellite and cable providers, allows the alerts to be propagated through the local broadcasters. In addition, the MCVP is required to carry the alert on other channels (programmed services) broadcast on the system. This requirement has evolved to cover Video on Demand and other video content. In a typical MCVP system, the alert will be distributed to every subscriber on the system.

Recent updates require broadcasters and MCVP systems to poll IPAWS for alerts as well as listening to two State or Local Primary broadcasters.

Federal regulations require the transmission of only four Event Codes (federally defined codes associated with the type of event in progress, such as flood watch, flood warning, tornado watch, etc.). The Presidential Emergency Alert Notification (EAN) and three test codes. All other codes are optional from a federal perspective but may be required or encouraged by individual state EAS plans. Local distribution of those additional codes is governed by the state EAS plan. Once an alert is triggered, it will be broadcast all at once to the entire area covered by a broadcaster or MCVP.

3.2.2 Wireless Emergency Alerts

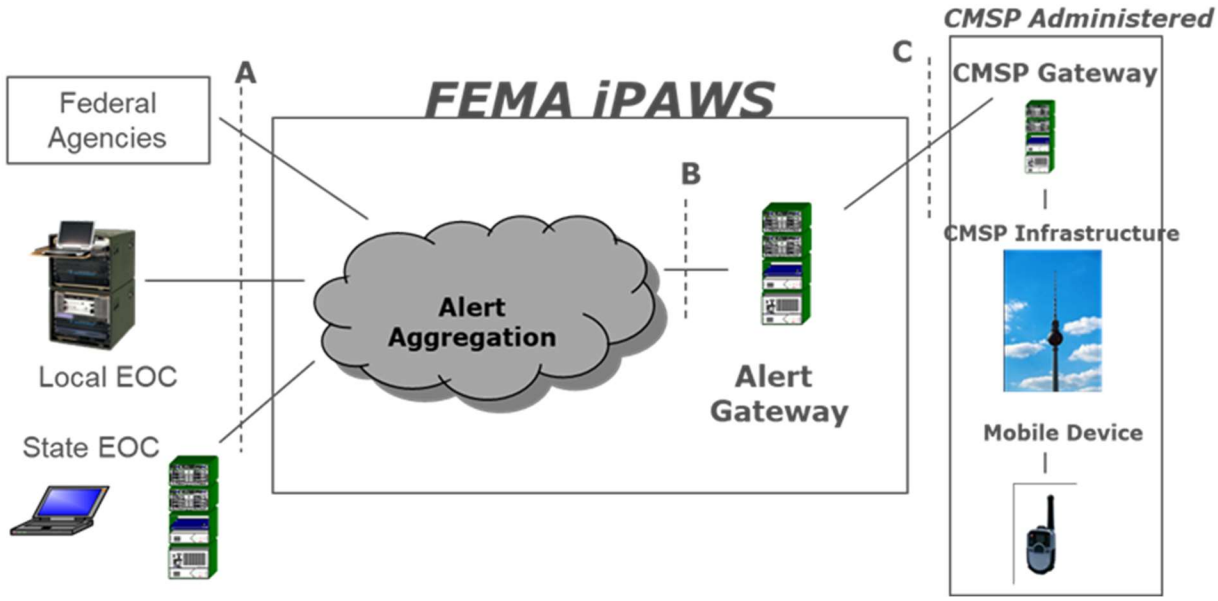

Figure 2 Wireless Emergency Alert System

The Wireless Emergency Alert system, launched in 2012, allows customers who own compatible mobile devices to receive geographically targeted alert information to warn them about imminent threats to safety in their area such as dangerous weather or other hazards, Public Safety information, or other critical situations, such as an AMBER Alert for missing children.

Authorized national, state or local government authorities may send alerts via IPAWS to the

participating wireless carriers. The wireless carriers then push the alerts to mobile devices in the affected area. All mobile devices will receive the alert over the broadcast; however, mobile device users may opt out of having any type of alert presented, with the exception of a Presidential Alert.

An alert is presented using alert tones (hearing), vibration (touch) and display (visual) means.

The alert is broadcast repeatedly over the indicated effective life of the alert, or until cancelled, to compensate for the mobility and radio aspects of the system. This ensures that as many users as possible in the broadcast area receive the alert, and that users not originally in the broadcast area should receive it within a short period of time after entering the broadcast area.

Alert Originators may initiate the following message types (See Section 4.2). Upon receiving any of these three message types, the actions taken by the Wireless Emergency Alert system are as follows

Alert:	This is a new alert to be broadcast. Upon receiving this command, the wireless carrier will initiate a new alert with the information provided.
Update:	This is an update to an active alert. Upon receiving this type of message, the wireless carrier network will perform the two-step action of cancelling the broadcast of the original alert, followed by initiating a new alert with the new information provided. If no associated active alert is found, only the second step of initiating the new alert will occur.
Cancel:	This cancels the referenced alert if still active. This means that the broadcast is discontinued. No information is presented on the mobile device concerning the cancellation.

3.2.3 Integrated Public Alert and Warning System

The figure below illustrates the full integrated system of alerts supported by IPAWS.

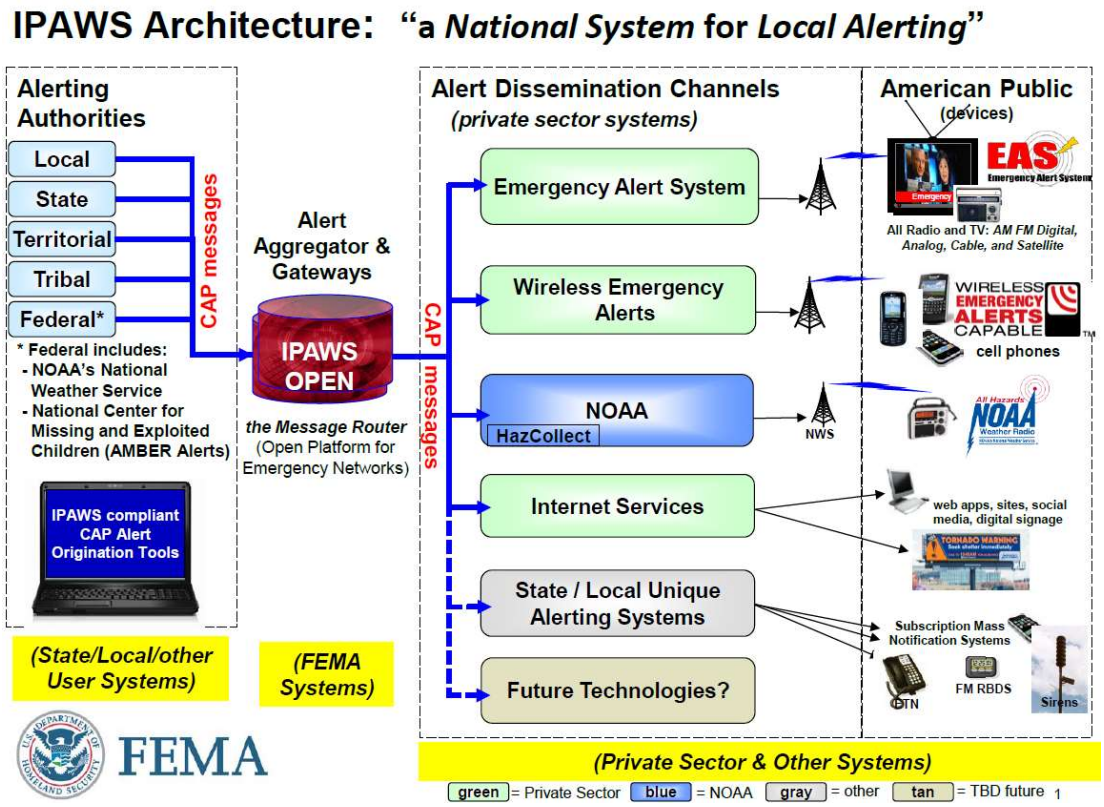

Figure 3 IPAWS Architecture[1]

"IPAWS provides public safety officials with an effective way to alert and warn the public about serious emergencies using the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), the National Oceanic and Atmospheric Administration (NOAA) Weather Radio, and other public alerting systems from a single interface. Federal, state, local, tribal and territorial alerting authorities can use IPAWS and integrate local systems that use Common Alerting Protocol (CAP) standards with the IPAWS infrastructure. View a list of IPAWS Organizations with Public Alerting Authority Completed in each state." From fema.gov, updated 4/29/2020.

[1] CAP Handler will replace HazCollect (NOAA) and is scheduled for deployment before the end of 2020.

4 Definitions and Acronyms

4.1 *Definitions*

Alert Originator: This is an entity authorized to create and send emergency messages.

Emergency Alert System (EAS): The Emergency Alert System was created as a successor to the Emergency Broadcast System as a mechanism to pass along a Presidential Alert and other optional types of alert in the case of a national emergency.

Integrated Public Alert and Warning System (IPAWS): IPAWS provides public safety officials with an effective way to alert and warn the public about serious emergencies.

Primary Entry Point (PEP): Primary Entry Points (PEPs) are the primary source of the initial broadcast for a Presidential Alert.

Wireless Emergency Alert (WEA): The Wireless Emergency Alert system allows customers who own compatible mobile devices to receive geographically targeted alert information to warn them about imminent threats to safety or other critical situations.

4.2 *Alert System Message Types*

Alert: new alert to be disseminated by the system

Update: updates the information for a previous alert

Cancel: cancels a previous alert

4.3 *Acronyms*

CAP	Common Alerting Protocol
EAN	Emergency Alert Notification
EAS	Emergency Alert System
FEMA	Federal Emergency Management Agency
GETS	Government Emergency Telecommunications Service
IPAWS	Integrated Public Alert and Warning System
MCVP	Multi-Channel Video Provider
NOAA	National Oceanic and Atmosphere Administration
NWS	National Weather Service
PBS	Public Broadcast System
PEP	Primary Entry Point
PII	Personally Identifiable Information
SECC	State Emergency Communications Committee
SFTP	Secure FTP
SLTT	State, Local, Tribal and Territorial
WEA	Wireless Emergency Alert
WPS	Wireless Priority Service

5 Tasks 1 and 2: Establishing and Maintaining Communications and Relationships Among Industry Stakeholders, Governmental Partners and Alert Originators

This section of the report will address communications among industry stakeholders for all types of alerts, with specific focus on EAS and WEA. It is important to note that the combined emergency alert ecosystem (EAS, WEA, Internet Services) includes stakeholders with varying capabilities and facing differing challenges. To this end, any recommendations must be flexible, so participants are able to develop solutions that work best for their individual situation. In this context, emergency alert systems (Systems) is used generically to refer to IPAWS alerts to include EAS, WEA, NOAA NWS weather and other present or future public alert systems.

All recommendations are completely outside the automated alert process and, therefore are intended to improve comfort and use of the system and will not have the effect of stalling or interrupting the automated process.

5.1 Background

Presently, both Alert Originators and stakeholders feel they are "out of the loop," but for different reasons. Alert Originators do not know if their alerts are received, processed and forwarded properly because there is no feedback, no verification from communication providers. Industry stakeholders also are out of touch. They do not always know when alerts have been issued and thus do not have insight into whether an issued alert has been properly processed and disseminated.

There currently is no official communication among the Alert Originators and industry stakeholders at the "people" level. Other than the "person" who physically triggered the alert, there is no further human involvement. It is all automated. There is no guidance on the appropriate action to take when/if someone detects a problem with an alert or the network. Alert Originators don't know if their alerts were received and processed. Additionally, industry stakeholders do not have insight into issued alerts, unless they happen to be located in the jurisdiction of the alert at the time that an EAS and/or WEA is issued, and see the alert in the same manner as the general public.

Systems are comprised of a wide variety of stakeholders, undertaking slightly different tasks, all directed toward the goal of providing rapid and widespread dissemination of alert messages. Each stakeholder has other duties and responsibilities toward their constituents and customers. In addition, all of these stakeholders encounter the same pressures and challenges of other businesses: competing priorities, employee turnover, technical upgrades, equipment failure/replacement, etc. These factors can combine to frustrate the efficient communication and operation of these Systems, or the development and maintenance of an effective working relationship.

5.2 Task 1: Establishing and Maintaining Communications Among Industry Stakeholders, Government Partners and Alert Originators

Task 1 offers best practices for establishing and maintaining communication among Alert Originators and industry stakeholders. To meet these goals the most basic elements are:

5.2.1 Harden the Network

Each stakeholder must maintain their network and the physical network connections (including broadcast connections) to the others that are required for effective and efficient delivery. The goal is to keep the physical System network working in all conditions. Best practices in this regard should include redundancy of pathways, standby power, batteries, diligent testing and all the other best practices associated with maintaining "always ready" physical networks.

While ensuring the physical network is always working, the state of the physical network is not part of the consideration of this question. Matters of a robust and hardened physical infrastructure are left to others. This section regarding physical infrastructure is included for completeness only.

5.2.2 Establish communications

By design, the Systems are automated. An alert originator pushes a button and a message is sent. That message is received, processed and forwarded without human intervention. This was more manageable when the original EAS network was limited to Alert Originators and a (relatively) few broadcast TV and radio stations. The landscape has changed. There are far more stakeholders in the network. Local and regional authorities of all manner and type can issue alerts. Cable operators add thousands of new stakeholders. WEA and Internet alerts increase that number further. The various stakeholders are not fully aware of all the others in the System. This makes it difficult to communicate information (other than the automated alert) to the rest of the stakeholders.

5.2.3 Provide Feedback

There is little reporting upstream to verify that alerts were received and processed. Nor do Alert Originators know if the alert they sent was received and processed as intended (no equipment or communications failures). A small amount of information sharing[2] is under development and not widespread. There is currently no way for a downstream stakeholder to question someone upstream about the relevance of an alert (for example, for a cable operator to question whether an Active Shooter alert is appropriate for their area) or to report a suspected breakdown in the network. This may be necessary in the event of a false alarm.

[2] Eyes on IPAWS description is included in section 5.3.1 Leverage Available Information.

5.2.4 Suggested Best Practices

5.2.4.1 Work with industry and the public safety community to consider what would be required to create a database of Alert Originators and industry stakeholders

A database of stakeholders would enable anyone in the "chain" to identify and communicate in either direction. There are a variety of reasons for this type of communication that include testing, reporting errors or system failures, education and collaboration, in addition to faster real time communication during emergencies.

Given the number and variety of stakeholders and the changing nature of the workforce, building and maintaining a database for Systems will be challenging. A database needs the following characteristics:

- DATA – Divide the data into two categories:
  - Essential – Limited to those items needed to communicate: company, name, phone number, email address, cell phone number for voice or text, and some identifier for the role they play (originator, cell provider, PEP site, etc.).
  - Desirable – Additional information that may be helpful to stakeholders to answer questions, share information and generally build relationships: job title, equipment/software deployed, physical address, education/experience, anything others may use to filter and select contacts to engage on relevant topics. We are confident that the future will present other opportunities to include additional participants and information.

- FLEXIBILITY – Provide information in a manner that enables users to filter, sort and select other stakeholders so they can focus on specific information or topics. For example, if a stakeholder desired information about how to program a specific piece of equipment, they should be able to identify other stakeholders with that equipment. Or, if a state or regional agency wanted to conduct a training session or convene a user group, they would need to be able to identify all of the stakeholders in that state or region.

- ACCESS AND USE - The database should be available to all stakeholders. They should be encouraged to use the database in creative ways to improve the Systems, expand their knowledge, improve relationships and identify new best practices. These opportunities may occur within stakeholder silos (one state agency with another) or across stakeholder silos (a PEP site with communications providers). This raises concerns about security that must be considered in the development, maintenance and use of the database.

- SECURITY – The database should not include any sensitive PII data. It is the responsibility of the database owner to prevent sharing of any data beyond the system boundary. Reference: The Privacy Act of 1974, 5 U.S.C. § 552a and the Federal Information Security Modernization Act of 2014.

- MAINTENANCE – Responsibility for creation and maintenance must be clear. It is important to note that any database is only as good as the information that is

provided and maintained. That requires careful consideration of the information requested and the structure of the database. It also requires a willingness on the part of the stakeholders to provide the original information **and** update that information when changes occur. For this reason, it is important to consider the entity that will be responsible for the creation and maintenance of the database. It cannot be left to volunteers.

FCC Action Item: Analysis is needed to determine the information already collected and accessible to begin building this database of Alert Originator and industry stakeholder information, as well as to determine the gap between this data and the complete set of data required as described in detail above. This responsibility could be a first step for the database administrator (see section 5.3.4). NOTE: This data falls into the two categories of Essential and Desirable. The Essential data addresses Task 1 as assigned to CSRIC VII . Desirable data represents additional data that complements the Task 2 recommendations by facilitating widespread knowledge of the capabilities of other stakeholders and their facilities, thereby enabling better sharing of technical and process knowledge, common practices, and a sense of community.

5.2.4.2 Create a central, real time reference that displays all System alerts.

A central reference for all alerts (national, regional, local) will enable any and all stakeholders to better understand what is happening anywhere in the nation (weather, fire, active shooting, etc.) and determine if they should prepare.

- The centralized resource for alerts needs to be dynamic so users can filter and analyze the data for their local or regional purposes.
- A centralized database of all alerts would allow data analytics to be conducted to better understand the number and nature of alerts, creating a positive feedback loop.
- A common data dictionary needs to be created and maintained to facilitate searching, filtering, and to drive data analytics.

5.3 Task 2: Developing and Maintaining Relationships between Communications Providers and Alert Originators

Only after effective communications have been created among the Alert Originators and industry stakeholders can we begin to develop and maintain relationships among those parties. Effective communication and strong working relationships are vital to ensuring efficient handling of every alert situation, especially stressful situations that require the level of confidence that allows personnel to respond quickly and decisively.

Task 2 offers best practices for developing and maintaining relationships between communications providers and Alert Originators. To meet these goals the most basic elements are:

5.3.1 Leverage Available Information

Currently, the Public Broadcast Service (PBS) sends every issued WEA over every public television transmitter, covering 95% of the United States. Through an initiative called "Eyes on IPAWS," developed at the request of emergency managers, stakeholders can view all WEAs issued in real time without internet access, using a television antenna and a broadcast receiver. Using broadcast technology, PBS disseminates the WEA messages in CAP format, which allows stakeholders to view richer content than what is displayed on a cell phone. "Eyes on IPAWS" is available for use immediately to view WEA messages and could eventually be used to provide an alternate source of IPAWS alerts once the centralized resource is created. This would provide redundancy of distribution for alerts.

FCC Action Item: "Eyes On IPAWS" is an example of connecting stakeholders to IPAWS alerts. A concerted effort to analyze the possibilities for expanding Eyes On IPAWS, or developing similar information sharing tools, to serve the entire emergency alert ecosystem is recommended. Stakeholders should be educated on the availability of the data and potential uses.

Eyes on IPAWS

Eyes on IPAWS is an information sharing tool under development by the Public Broadcasting Service (PBS) that allows all stakeholders to view all WEAs in real-time, including active and expired alerts. PBS and its member stations are already integrated as a key component of the WEA system, providing a national over-the-air feed of all WEAs as a robust, redundant alert source available to wireless carriers. PBS has leveraged its WEA feed to create Eyes on IPAWS, with the goal of providing stakeholders with increased knowledge and transparency of issued alerts. Sourced directly from IPAWS, the alerts are delivered over broadcast airwaves by local PBS member stations and are not subject to network congestion or typical outages. Alert Originators, emergency managers, and any other stakeholders can use Eyes on IPAWS to determine active WEAs nationwide; confirm transmission of issued WEAs; gain awareness of WEAs issued by other agencies; view alerts based on location, alert type, or date; and analyze the impact of WEAs using the data from Eyes on IPAWS in after-action analysis.

PBS provides insight into live WEAs today via the website warn.pbs.org, which displays all active WEAs in real-time on a map. This free service is meant to serve as a validation tool for Alert Originators to confirm transmission and geographic distribution of WEAs.

Given that WEAs are intended to inform specifically of imminent threats to life and safety, awareness of WEAs is uniquely valuable to emergency managers and first responders. With sufficient demand for the service and financial support to execute the program, PBS has the potential to expand its national feed to include the IPAWS All-Hazards Information Feed, which would provide this visibility into all other alerts issued by IPAWS as well.

5.3.2 Encourage Automated Verification

As alert signaling is passed along the end-to-end system, acknowledgements to indicate successful processing or errors may be exchanged between any two signaling points. Any error conditions received in the response from a downstream stakeholder should be relayed back to the originating party.

Automated verification of alert reception and processing will enable Alert Originators and stakeholders to analyze the results of alert messages and tests to constantly improve the effectiveness of the system. IOT makes this seem very plausible. The bigger questions are who will examine the data and will they have the authority to act upon it.

FCC Action Item: Encourage stakeholder software updates that support real-time awareness of error conditions by the Alert Originators. Error conditions received in the response from a downstream stakeholder should be relayed back to the originating party.

5.3.3 Implement the Database

A database is of no value unless it is maintained and utilized. The party responsible for the database should develop and implement a program to regularly communicate with all participants. These programs should have sufficient flexibility to accommodate varying markets, geography and participants. The focus of this activity can include encouraging industry stakeholders to participate in several ways. All of them will both enhance the relationship among the stakeholders and reinforce the network's resilience.

5.3.4 Establish Ownership

Each stakeholder must ensure their local equipment is working properly to fulfill their role in the System message chain; making sure messages are delivered along the entire System. The goal is to make sure that the specific System equipment is performing as expected; receiving, processing and forwarding the correct information. Each stakeholder is responsible for ensuring that the equipment under their control is installed properly, provisioned/programmed properly (including updates) and is overseen by an individual qualified and trained to operate it.

Each stakeholder must specifically assign these responsibilities to someone who is aware of the need for diligent testing and monitoring to make sure all equipment is working properly within the System as a whole. This includes ensuring that replacement equipment is properly programmed/tested when installed.

- Identify (specifically) and engage the people responsible for the network's maintenance and operation, develop a sense of ownership at the local level, create relationships among participants for the sharing of ideas, and provide a structure for the flow of information.
- Encourage user groups. Best practices in this regard include:
  - Training on the importance of the entire System,
  - Regional training, workshops and proficiency exercises to ensure readiness and a comfort level among personnel to handle routine or non-routine circumstances efficiently.
  - Individual local equipment training,

- Regular information to stakeholders (updates, newsletters, information regarding changes), reminders to conduct internal tests, maintaining logs of System monitoring, installing (whenever possible) automated monitoring/alert systems for critical equipment.
- Regional in-person meetings among stakeholders to discuss issues relevant to the Systems and network (user groups) can help create a greater sense of ownership and participation as well as improve knowledge of best practices.

FCC Action Item: Consider what would be required to create an independent central database of alert originator and industry stakeholder contact information, including identifying costs, determining the best approach to administration (including providing oversight to ensure consistency and security), and determining an appropriate administrator.

6 Task 3: Effective Alternate Lines of Communications

Similar to having multiple methods to access information before, during, and after an emergency, it is critical to establish multiple lines of communication with key industry stakeholders and partners to enable consistent messaging and align collaboration. Capturing these measures and standard operating procedures from both a communication and telecommunication standpoint fosters an approach that meets the needs of a community when it matters the most.

6.1 *Communications Strategy and Protocols*

When disasters occur, effective communication must continue through the entire value chain. Having a communication strategy and plan in place well ahead of an event will help promote timely and accurate exchange of information between stakeholders and to the public as emphasized in the Department of Homeland Security "Ready Campaign – Crisis Communications Plan" (https://www.ready.gov/business/implementation/crisis).

Stakeholder Recommendations for Effective Communications:

- Conduct an analysis of current methods used to reach partners and communities.
- Conduct an analysis of, validate and catalog best communication practices.
- Employ redundant means to communicate with partners and communities during emergencies through the most effective means at their disposal. These means can include mobile, chat applications, radio, and/or satellite broadcast service such as satellite phone systems.
- Identify authorized officials to the public to reduce the impact of those who may not be following one of the official sources of information
- Improve the ability for approved authorizing officials to amplify messaging and communication of critical information through multiple means such as social media, broadcast community, and federal agency delivery services such as NOAA Weather Radio.
- Establish protocols and strategy for Social Media dissemination of alert information to the public. This includes working with providers of RSS based alerts, such as Google and Facebook.

6.2 *Alternate or Expanded Communications Paths*

For stakeholders to engage with each other effectively, underlying technology and alternate communication methods must be in place. Stakeholders must be prepared to recognize when the situation calls for alternate or additional communications paths to continue the flow of information when seconds count. They must also strive to ensure that the information communication to the public is consistent.

Recommended stakeholder actions to provide a framework to ensure the consistency and coordination of messaging prior to public release:

- Conduct risk evaluation and testing of their telecommunications infrastructure (VOIP vs POTS etc) on a regular basis.
- Implement continuous monitoring of telecommunications to ensure system integrity, for example a "keep alive" message.
- Apply for SFTP Priority 3 (public health, safety, and law enforcement) or Priority 4 (public services/utilities, public welfare, and entities performing critical infrastructure protection functions) access to GETS and WPS services, and periodically confirm the ability to access these systems.
- Implement procedures to ensure the onboarding and departures of stakeholders are maintained and updated, as needed.
- Complete periodic revalidations to ensure that all records for SFTP access to GETS and WPS records are accurate.
- Establish a Security and Access Control Plan (Physical security of facility and equipment, role-based access restrictions)
- Establish standard operating procedures in coordination with all partners to ensure consistency and coordination of message content and timing.
- Investigate possible technology interoperability including cross-jurisdictional alerting among stakeholders' equipment for more efficient and error-free dissemination into coordinating systems.
- State Emergency Communications Committees (SECCs) to establish strategy for Social Media directed towards State, Local, Tribal, and Territorial (SLTTs) Governments to provide updates or coordinate activities that apply to a large scale Physical mediums (e.g., sirens, public address systems, etc…), preferably on systems not affected by interference. Stakeholders need to address the accessibility[3] of alerting products and give consideration to multilingual populations.

[3] Resources with tips for providing notification to people with disabilities or limited English proficiency:
- Americans with Disabilities (ADA) Best Practices Tool Kit for State and Local Governments - https://www.ada.gov/pcatoolkit/chap7emergencymgmtadd1.htm
- FEMA Alerting the Whole Community - People with Disabilities and Others with Access and Functional Needs Fact Sheet - https://www.fema.gov/media-library-data/1465326408751-bb57c7fa64f8ede2d615439dc1e3d6db/Alerting_the_Whole_Community_ADA_2016.pdf
- Department of Health and Human Services: Ensuring Effective Emergency Preparedness, Response And Recovery For Individuals With Access And Functional Needs Checklist For Emergency Managers - https://www.justice.gov/crt/file/885396/download
- Federal Coordination and Compliance Section, Civil Rights Division, U.S. Department of Justice: Tips and Tools for Reaching Limited English Proficient Communities in Emergency Preparedness, Response, and Recovery (2016) - https://www.justice.gov/crt/file/885391/download
- Limited English Proficiency (LEP): Emergency Preparedness - https://www.lep.gov/emergency-preparedness

7 Task 4: False Alert Prevention and Corrective Actions following a False Alert

As illustrated by recent events such as the false alert in Hawaii, it is critical for Alert Originator personnel to prepare for handling the aftermath of a false alert. This will involve many internal activities, however, the key activity that we focus on here is the follow-up with a cancellation and/or an update.

False alerts have the potential to produce widespread negative impacts no matter how quickly and efficiently the agency performs the follow-up to correct the situation. Practices to prevent the sending of false alerts should be reviewed and recommended for adoption.

This section of the report focuses on recommendations for both the prevention of, and reaction to, the sending of false alerts.

FCC Action Item: Review Sections 7.1-7.3 and recommend for incorporation into Alert Originator Standard Operating Procedures.

7.1 Types of False Alerts Considered

The false alert scenario on which the FCC has focused for this task is the case where the alert text is describing a situation or emergency that does not exist. Another case discussed while forming the recommendations described below is a scenario in which the alert text is correct, but could be mistakenly paired with incorrect geographic information describing the alert area. While the alert content in this case is a true description of an existing situation or emergency, it is effectively the same as a false alert from the perspective of the people it reaches but to whom it does not apply. Similar procedures to those of retracting/correcting a false alert would need to follow in order to notify the original recipients of the error, as well as to quickly and efficiently send a new alert to the correct alert area. The recommendations in this report were written with both of these types of "false" alerts in mind.[4]

[4] Note, the case of presentation of the alert on mobile devices beyond the alert area, commonly referred to as "overshoot", is not part of the consideration for these recommendations. Overshoot is a result of broadcast coverage patterns that may extend beyond the edges of the defined alert area.

7.2 Recommended Practices for Preventing False Alerts

Regardless of the actions taken to retract or correct a false alert, there is still a risk of spreading panic or even a crisis situation resulting from the initial moments of having the public receive a false alert. Policies and best practices put in place to prevent the sending of a false alert are essential in any alert agency.

False alerts may be sent by accident, such as the case in which Hawaii when a test alert is mistakenly sent on a live alerting environment. There could also be inaccurate information communicated to the alert agency, either intentionally or unintentionally. The following recommendations are intended to address all of these possibilities.

7.2.1 Minimize Human Error

Practices should be put in place to minimize errors that may result from human intervention in highly alarming circumstances. Additional prompts should be required to confirm the intent to initiate the alert. This level of alert should also require a multi-person initiation structure that includes at least one of the supervisory level personnel if this additional step can be added to the operating procedures and performed in such a way as to be effected in a timely enough manner to avoid a critical delay in dissemination.

7.2.2 Separate Test and Live Alert Environments

The public should never be in a position to mistake a test alert for an actual alert. In order to avoid sending a test alert to general public, there should be physical separation between the live alerting environment and the closed-circuit test environment. If physical separation is not practical, separate entry sequences should be available in the software. In case a test alert does manage to reach the live alerting environment, further protection should be practiced in the form of prefacing, and preferable also concluding, the test alert text with appropriate wording to clearly indicate that a test is being conducted. This will ensure that recipients will understand that this is only a test.

FCC Action Item: It is recommended that the FCC consider initiating a rulemaking to require the inclusion of text in test alerts to indicate that a test is being conducted.

7.2.3 Security Access and Control Plan

Agencies must insure a secure environment through a Security and Access Control Plan. This should include the physical security of the facility and equipment, as well as role-based access plans. Personnel should confirm the location of all physical credentials and update electronic credentials on a regular basis, with intervals not to exceed 90 days. Any churn in personnel should trigger an additional round of verification. The live alerting environment should require a higher level of validation, such as two-factor authentication.

7.2.4 Training

The wide variety of processes within the industry increases the possibility of mistakes when personnel move between facilities. Consideration of some uniform elements in the workflow to facilitate standardized training and ease of moving between facilities is recommended. Regular training, workshops and proficiency training exercises are required to ensure readiness and a comfort level among personnel to handle routine or non-routine circumstances efficiently.

7.2.5 Validation of Imminent Danger Alerts

Some alerts may be triggered by equipment registering specific circumstances and this information is received over a secured link, while other alerts may originate from incoming calls or other sources. While speed of alert dissemination is critical in many cases, verification of that alert, possibly even in parallel with the process of triggering the alert, may be prudent. This is especially applicable to any alarming types of alerts which could result in a panic situation. While the process to trigger the alert is in progress, personnel not involved in that process have the opportunity to reach out to the party from which the alert came, either confirming the source, confirming their authority as a source, or both. In some cases, reaching out to alternative parties for corroboration of the alert information will be necessary.

All agencies should determine which alert types, sources, or a combination of those factors should result in parallel verification procedures. In the case that the verification procedure may take longer than triggering the alert, next steps for retracting the alert need to quickly follow.

7.3 *Recommended Practices for Recovery following the sending of a False Alert*

In the event that a false alert occurs, the actions taken by the alert agency following the false alert, and the speed and accuracy with which they are taken, are critical to limiting the negative impacts to the public, as well as limiting the spread of the false information. The more time that passes, the further the false alert information can spread by word of mouth or other means.

Recognize the differences between EAS and WEA

EAS and WEA systems have different structures and capabilities. The systems also have different speed of dissemination. The slower dissemination of EAS introduces the possibility of different impacts to user presentation in the case of triggering multiple active alerts over a short period of time. While the prevention of false alerts may be very similar in both cases, allowing for the common set of recommendations above, the steps taken to recover from a false alert are quite different. The training for any personnel, especially for those with access to both systems, must be thorough as to the differences in the capabilities and reactions of these systems to specific commands.

The message types and responses of the two systems are summarized in the following table. Further context and detail can be found in the individual sections for each type of system below.

Message Type	WEA	EAS
Alert (new alert)	A new alert is created: repetitive broadcast begins and continues through indicated lifespan of the alert.	A new alert is created which traverses the system and is broadcast at all broadcast points one time (no repetition).
Cancel	Broadcast for the referenced alert ceases.	No action taken if the alert has already been broadcast.
Update	Broadcast for the referenced alert ceases and a new alert is created.	Response is the same as to the Alert message type. A new alert is created which traverses the system and is broadcast at all broadcast points one time (no repetition).

Table 3 - Impact of each Alert Action for WEA and EAS

FCC Action Item: Any personnel with access to both WEA and EAS for sending alerts should be required to have training that clearly explains key differences between the two systems and the difference in alert handling that will result from each of these key actions.

7.3.1 Wireless Emergency Alerts

Following the dissemination of a false WEA, there are many factors to consider when sending an Update or a follow-up alert.

7.3.1.1 Choose Initial Steps Wisely

The critical initial step is to stop the sending of false information in order to limit, to the extent possible, the number of people that it may reach. Upon receiving a new Alert, the WEA system broadcasts an alert periodically throughout the designated life of the alert in order to reach mobile devices that either did not originally receive the broadcast due to a radio anomaly or other circumstance (e.g., inside an elevator) or were outside the broadcast area but are moving into the that area.

There are two actions that an Alert Originator may take in order to stop the broadcast of a false alert. The Alert Originator can send an Update which includes new information, in which case the wireless carriers' systems will perform a two-step process to first cancel the broadcast of the original alert, then begin sending a new alert with the new information. The other option for the Alert Originator is to send a Cancel, for which the only resulting action is to cease the broadcast. No further information will reach the mobile device in the event of a Cancel. In other words, the mobile device will not present information to the user concerning the cancellation of the alert.

Time will be required to perform checks, gather all needed information and approvals, and to formulate an appropriate follow-up message to retract and possibly explain the false alert information. With this in mind, the recommendation for required steps to be taken following a false alert:

> Step One: Send an immediate Cancel to cause the wireless system to cease the broadcast of the false alert information.
>
> Step Two: Follow as quickly as possible with a new alert with additional information or instructions to communicate the current situation.

An exception to this recommendation applies if the Alert Originator has the ability to send an immediate (e.g., automated single-touch or similar) Update with a simple message indicating the cancellation of the referenced false alert. The benefit of performing this alternative to Step One above would be that in addition to ceasing the broadcast, the users receiving it would know of the cancellation, hopefully preventing further spreading (e.g. word of mouth). The second step would still be required to fully communicate the current situation.

FCC Action Item: The ability to allow the Alert Originator to initiate a near-instant Update in a manner that both stops the broadcast of the false WEA and reaches the mobile devices with a message indicating that the alert was cancelled is in use, but not widespread use. It is recommended that vendors for Alert Originators be strongly encouraged to have similar functionality available.

7.3.1.2 Audience for the New Alert Information

Alert Originators should attempt to avoid confusion by formulating the new alert message keeping in mind that the updated information should be informative enough to indicate to any new mobile devices receiving it that a false alert is being retracted.

7.3.1.3 Coverage Considerations for Update

The updated information, whether sent in an Update or new alert, should be triggered from the same Alert Originator to ensure similar dissemination. Keeping in mind that this is a mobile system, meaning that some mobile devices may have left the original broadcast area by the time the new information is available over the broadcast, Alert Originators should consider whether enough time has passed that it would be beneficial to slightly enlarge the defined broadcast area (in the case of a geometric shape definition) in order to communicate this information to these outbound mobile devices.

Given that information may spread by other means by the time that an Update or new alert can be triggered, Alert Originators should use additional means of media or other resources already documented as part of their false alert recovery process.

7.3.1.4 Training

False alerts not only have the ability to create a panic in the public domain, they may have this impact in the Alert Originator facility. Regular workshops and proficiency training exercises should create a sense of confidence in agency personnel with respect to their ability to properly recovery from this type of error. Consideration of some uniform elements in the workflow to facilitate standardized training and ease of moving between facilities is recommended.

7.3.2 Emergency Alert System

Following the dissemination of a false EAS message, there are many factors to consider when sending an Update or a follow-up alert.

7.3.2.1 Distribution of the Updated Alert Information

The final alert distribution, or specific set of endpoints where it is broadcast, depends on the Event Code used. If a false alert is triggered, a subsequent alert to correct the information in the erroneous first alert must use the same Event Code as the first message. This is to ensure it will be treated (filtered) in the same manner as the original alert, thereby using that same distribution.

- A CAP "Cancel" message may be sent. However, Alert Originators must understand that a Cancel message will only prevent messages (received by CAP) that have not yet been transmitted by the EAS device at an EAS Participant location. A CAP Cancel will

have no effect on a CAP EAS message that has already been transmitted. Likewise, a CAP Cancel will have no effect on a message that is in the legacy EAS system.

- A CAP "Update" is viewed by the Emergency Alert System as a new alert, and will be treated the same as a new alert.

If an alert is sent erroneously, the sender must consider that word of that alert may have spread by word of mouth or other means. Additional corrective information must be provided quickly to local broadcasters and news organizations. Alerting local public safety and government officials is also highly recommended. Depending on the alert, consideration should be given to alerting other authorities such as local hospitals or clinics.

7.3.2.2 Address all Capabilities within EAS

The Emergency Alert System is a dual system, using both Internet-delivered CAP and broadcast EAS relay paths, with the EAS relay path having limitations that don't apply to the Internet-delivered CAP path. The CAP version of the message can include more information (specifically, in this case of a retraction or correction of a false alert). The EAS version of the message may contain significantly less information, due to the constraints of the EAS Protocol.

- If a follow-up message is sent via conventional EAS protocol (rather than CAP), Alert Originators must note that the text display to the public (over video TV and cable systems) will contain standard alert text information. There will be no additional information to indicate the follow-up message is a cancellation or retraction of a previous message.
- Likewise, if a follow-up message is sent via CAP, there is a significant possibility that the more informative EAS text inside the CAP message will be truncated somewhere along the distribution chain, removing the chance of clarifying the situation for the recipient.
- Example: If an originator suffers a false Radiological Hazard Warning and sends a follow up message over EAS, this could result in the same alert text string as for the original false alert being displayed over video systems: "A civil authority has issued a Radiological Hazard Warning for the following areas: xxxx). Unless the EAS device picks up the CAP message first (which happens about 50% of the time), the TV/MCVP textual display resulting from the follow-up alert will be as misleading as that of the false alert.

7.3.2.3 Training

The best practice is to ensure that false or erroneous alerts are not sent in the first place; however, if one is sent, then senders should be aware of what is required to provide corrective action. It is recommended that regular workshops and proficiency exercises be held for personnel responsible for generating alerts. A check list to help senders think through who else should be notified should be included in this training.

7.3.2.4 Additional Measures

It is also recommended that Alert Originators and state and local emergency communications committees ("EAS Committees") encourage local EAS Participants in their area to enable a capability called Triggered CAP Polling™ on their EAS devices. Having this capability will enable EAS Participants to immediately retrieve the more informative CAP message, even if a shorter EAS message is received first.

8 Conclusions

Recommendations and next steps included in this report will continue to improve the current alert systems by assisting all personnel in their tasks and supporting their ability to reach out, work as part of a greater team, and share knowledge. The recommendations for false alert handling will decrease stress in both the alert personnel and public by reducing the number of false alerts and bringing a more automated structure to the reactions following a false alert.

9 Recommendations

The following recommendations are made to the FCC by CSRIC VII:

- Analysis is needed to determine the information already collected and accessible to begin building a database of Alert Originator and industry stakeholder information, as well as to determine the gap between this data and the complete set of data required as described in detail above. This responsibility could be a first step for the database administrator (see section 5.3.4). NOTE: This data falls into the two categories of Essential and Desirable. The Essential data addresses Task 1 as assigned to CSRIC VII. Desirable data represents additional data that complements the Task 2 recommendations by facilitating widespread knowledge of the capabilities of other stakeholders and their facilities, thereby enabling better sharing of technical and process knowledge, common practices, and a sense of community.

- "Eyes On IPAWS" is an example of connecting stakeholders to IPAWS alerts. A concerted effort to analyze the possibilities for expanding Eyes On IPAWS, or developing similar information sharing tools, to serve the entire emergency alert ecosystem is recommended. Stakeholders should be educated on the availability of the data and potential uses.

- Encourage stakeholder software updates that support real-time awareness of error conditions by the Alert Originators. Error conditions received in the response from a downstream stakeholder should be relayed back to the originating party.

- Consider what would be required to create an independent central database of Alert Originator and industry stakeholder contact information, including identifying costs, determining the best approach to administration (including providing oversight to ensure consistency and security), and determining an appropriate administrator.

- Review Sections 7.1 – 7.3 and recommend for incorporation into Alert Originator Standard Operating Procedures.

- Recommend that the FCC consider taking steps to initiate a rulemaking to require the inclusion of text in test alerts to indicate that a test is being conducted.

- Any personnel with access to both WEA and EAS for sending alerts should be required to have training that clearly explains key differences between the two systems and the difference in alert handling that will result from each of these key actions.

- The ability to allow the Alert Originator to initiate a near-instant Update in a manner that both stops the broadcast of the false WEA and reaches the mobile devices with a message indicating that the alert was cancelled is in use, but not widespread use. It is recommended that vendors for Alert Originators be strongly encouraged to have similar functionality available.