

Before the  
**Federal Communications Commission**  
**Washington, D.C. 20554**

In the Matter of )  
 )  
Amendment of Part 11 of the Commission's Rules ) PS Docket No. 15-94  
Regarding the Emergency Alert System )  
 )

**COMMENTS OF TRILITHIC, INC. IN RESPONSE TO FCC NOTICE OF  
PROPOSED RULEMAKING**

**1. INTRODUCTION**

Trilithic, Inc (“Trilithic”) hereby responds to the Commission’s Notice of Proposed Rulemaking in the above-captioned proceeding.

## 2. PRESIDENTIAL ALERTS FORMATTED IN CAP

**Trilithic is concerned that a CAP formatted EAN with a streaming audio resource may not be processed correctly by all EAS equipment. The type of streaming audio that will be used and the method used to terminate the alert must be defined more clearly before interoperability can be guaranteed.**

Within ¶49 of the NPRM, the FCC seeks comments on removing the restriction that Presidential Alerts can only be formatted in the EAS protocol. The ECIG CAP to EAS Implementation Guide specifies that the audio will be an MP3 stream received as an HTTP progressive-download or from an HTTP streaming MP3 server. This definition is too broad and does not provide enough information to perform tests that will ensure compatibility with a CAP formatted Presidential Alert originated by FEMA. Trilithic has tested its EAS Encoder/Decoders with different types of streaming audio, but without knowing the type of streaming audio that will be used these tests can only be considered a best-effort and do not guarantee compatibility. While we understand the desire to avoid placing too many limitations on the streaming audio so that new more efficient and effective technologies can be used as they become available, adequate specifications must exist to ensure interoperability.

An EAN can have an indefinite duration, and when received from a traditional EAS source the rules clearly specify that an EOM will be sent to terminate the alert. In the case of a CAP formatted EAN with streaming audio, the rules do not describe the termination method. There are some logical methods that can be used, like the end of the audio stream or upon receipt of a CAP formatted cancellation message, however the rules should clearly

specify the termination method in order to ensure compatibility. Trilithic has tested different methods for terminating a CAP formatted EAN, and it's worth noting that depending on the type of streaming audio used, detecting the end of the stream is not always readily apparent and an inactivity timeout may be required, which can result in several seconds of silence.

Trilithic recommends that a test of a CAP formatted Presidential Alert be conducted by FEMA to ensure proper operation of EAS equipment, and anytime the process or the type of streaming audio is changed, additional tests be conducted. Live testing is not necessary. It can be accomplished in a lab environment or using the IPAWS-OPEN test feed, as long as all EAS manufacturers are given the opportunity to verify proper operation of their equipment.

### **3. LIVE CODE TESTING**

#### **a. Benefits**

**Trilithic believes that live code tests will provide more accurate verification that specific alerts will reach the intended audiences by providing testing conditions that more accurately represent actual emergency conditions.**

Within ¶61 of the NPRM, the FCC seeks comments on the benefit of using live code tests and if they would provide a more realistic verification of specific alerts. EAS equipment, and downstream equipment used for presenting emergency information to the public, can be configured and setup differently for each type of alert. The use of live code tests will verify proper configuration and operation of all equipment used to present a specific alert to the public.

b. Notification & Outreach

**Trilithic believes that public notification and outreach is very important to avoid confusion between live code tests and real emergencies.**

Within ¶62 of the NPRM, the FCC seeks comments regarding the steps that EAS stakeholders could take to minimize any public confusion that may result from live code testing. The audio message included with a live code test can specify that the alert is "only a test", however only alerts received from CAP sources are capable of including text to visually indicate that the alert is a test. Live code tests received from traditional EAS sources will not include a visual indication that the alert is a test.

c. Accessible Live Code Testing

**Although CAP formatted messages can visually indicate that an alert is “only a test”, any alerts received from traditional EAS sources will not include a visual notification.**

Within ¶71 of the NPRM, the FCC seeks comments regarding whether accessible video crawl or full-screen replacement slide would be sufficient to overcome the public’s preconception of the meaning of the Attention Signal and if persons with disabilities benefit from concepts such as color-coded messages. Only CAP formatted alerts are capable of including text to visually indicate that the alert is a test, or to indicate a category for the alert. When EAS equipment receives a live code test from a traditional EAS source, the CAP text will not be displayed for viewers and an alert category will not be present to indicate a unique color for the test. Additionally, displaying different background or border colors based on the category of the alert is

not currently supported by much of the equipment used to display alert information and would require many EAS Participants to make large expenditures for the purchase of updated equipment, and possibly architectural changes, to support these features.

#### **4. CABLE FORCE TUNING AND SELECTIVE OVERRIDE**

##### **a. Technological Advancements**

**Trilithic believes that force tuning is still the most cost effective method for many MVPDs to present EAS messages to their subscribers.**

Within ¶81 of the NPRM, the FCC seeks comments on whether technology has advanced to the point where selective override on a channel-by-channel basis can be readily programmed into cable equipment without imposing undue burden on cable providers. The most common protocol used to deliver EAS messages to downstream equipment and STBs is SCTE-18 (ANSI J-STD-42-B). This protocol supports a list of exception services to identify channels that should not be affected by an EAS message. Although Trilithic EAS Encoder/Decoders have supported the list of exception services since the SCTE-18 protocol was first deployed, there may be technical difficulties related to implementation that would be best addressed by MVPDs.

Within many cable systems, force tuning is often the most cost effective and efficient method to present EAS messages on all channels within the system.

If force tuning was no longer allowed, Trilithic believes that the cost of adding and replacing equipment to override the audio and video on each individual channel would impose an undue burden on MVPDs.

b. Delivery of EAS Messages through Different Platforms

Within ¶83 of the NPRM, the FCC seeks comments on whether there are or can there be any differences between the EAS messages that consumers see when viewing the alert on broadcast channels versus cable channels. EAS messages transmitted by MVPDs and local broadcast channels should have the same audio and text content. Although the presentation of these messages may look different because broadcast channels tend to overlay text crawls onto their programs and MVPDs usually perform a full-screen replacement, the delivered audio and text content of the EAS message should only differ based on whether the alert is received from a CAP source or a traditional EAS source.

## 5. TECHNOLOGICAL POTENTIAL FOR IMPROVEMENTS IN ACCESSIBILITY

**Trilithic does not recommend the use of machine-generated translation for emergency alert information and believes that support for multiple languages should occur at origination points where operators can create audio and text content in languages for the desired audience.**

Within ¶94 of the NPRM, the FCC seeks comments on using machine-generated translations for providing emergency information in non-English languages. While technology exists to translate text into different languages, and to convert the text into audio, the machine-generated translations are not be as understandable as a message

written or spoken by a human. In the case of emergency messages, the results of a bad translation could be disastrous.

Support for multiple languages can be accomplished more accurately and effectively at the origination point, where a human can create audio and text content in languages for the desired audience, rather than translations at every EAS Participant site. If automated translation technology is employed, there are several compelling reasons why it should occur at the origination or aggregation points. Origination points are closely monitored whereas automated broadcast and MVPD sites may not be. Such a requirement by thousands of end devices would be less cost effective than adoption by hundreds of origination or tens of aggregation sites. Also, originators are more likely to get meaningful feedback on the translations and make corrections as necessary.

## **6. ALERT AUTHENTICATION**

### **a. Discarding CAP Messages with Invalid Signatures**

**Trilithic recommends that CAP messages with invalid signatures that are received from IPAWS-OPEN should be discarded. However, Trilithic also believes that the methods involved in securing CAP messages against malicious actions for other CAP sources should be left to the states and localities that implement CAP.**

Within ¶136 of the NPRM, the FCC seeks comments on requiring CAP messages with an invalid signature to be discarded. Trilithic EAS Encoder/Decoders provide the option to discard CAP messages with a bad digital signature or to retransmit the alert and log a warning that the signature verification failed. Trilithic supports the idea that CAP messages from IPAWS-OPEN should be discarded if and when they

contain a bad digital signature. This is justifiable because the IPAWS system already requires messages to be signed before they can be aggregated. However, requiring all CAP formatted messages to be digitally signed may be counterproductive since there are many ways to secure digital communications. Additionally, maintenance of cryptologic keys for all CAP services, originators, and consumers may be unnecessary overhead that would prove difficult to maintain.

b. Adding Authentication Data to EAS Protocol Formatted Messages

**Trilithic is not in favor of adding a unique ID or authenticator ancillary to the audio portion of an EAS message. Trilithic believes that this method of authentication would reduce reliability and could potentially result in corruption of authentication data which could cause valid messages to be rejected. Additionally, this would reduce the amount of time available for audio messages and require costly hardware replacement for both consumers and service providers.**

Within ¶137 of the NPRM, the FCC seeks comments on adding authentication data to EAS Protocol-formatted messages. It is worth noting that the proposed authentication methods would only have prevented the two false activations cited in this proceeding which were retransmissions of previous alerts. The other false activations were originated with EAS Encoders, which (presumably) would have included the correct authentication data, and therefore activated downstream EAS equipment.

Trilithic is not in favor of adding a unique ID or authenticator ancillary to the audio portion of an EAS message. It would reduce reliability because the FSK data carrying the authentication information could not utilize the same integrity check

used for EAS Protocol header codes, where a two out of three match is required. It could result in corruption of the authentication data and in turn cause valid emergency messages to be rejected. It would also reduce the amount of time available for a voice message, which contains the specific details for EAS Protocol-formatted messages. Older EAS equipment and NOAA receivers would not likely support such a requirement, resulting in widespread and costly hardware replacement for both consumers and service providers. Equipment that can be updated would likely require significant development cost and time to implement these features.

c. Virtual Red Envelope (VRE) System

**Trilithic does not support adopting the proposed VRE solution for authenticating EAS Protocol-formatted messages. It would not have prevented many of the cited false activations, and could prevent older EAS equipment and NOAA receivers from functioning properly. For these reasons, we do not feel that the benefits outweigh the costs.**

Within ¶138 of the NPRM, the FCC seeks comments about a Virtual Red Envelope (VRE) solution to EAS alert authentication that could be applied to alerts formatted in the EAS Protocol. Trilithic does not support adopting the proposed VRE solution for authenticating EAS Protocol-formatted messages because it will not prevent all false activations and will require changes to the EAS Protocol header codes. Any change to the EAS Protocol header codes will require changes to the EAS equipment's FSK Processing, which is one of the most critical operations, and could adversely affect the hardware of some devices. Changing the EAS header

codes could also prevent older EAS equipment and NOAA receivers from functioning properly.

Furthermore, the suggestion that messages can be manually verified if the VRE authentication fails is unworkable for many systems and is contrary to automatic operation, which is an important capability of the EAS. Many systems setup their EAS equipment to automatically forward alerts, and they do not have the personnel or processes available to manually verify alerts.

The VRE solution would not prevent false activations such as the Zombie attack hoax or the false EAN from WBLE, because an EAS Encoder was used to originate these messages and so the correct authentication code would have been present. Older EAS equipment and NOAA receivers would not likely support such a requirement, resulting in widespread and costly hardware replacement for both consumers and service providers. Equipment that can be updated would likely require significant development cost and time to implement.

d. Suggestions for EAS Message Authentication

**If an authentication method is added to EAS Protocol-formatted messages, Trilithic proposes to replace the "LLLLLLLL" station identification with the authentication data in an alpha-numeric format to provide backwards compatibility, reduce development costs, and shorten deployment time.**

If any authentication method is added to EAS Protocol formatted messages, Trilithic recommends a vendor-neutral replacement of the "LLLLLLLL" station identification with the authentication data in an alpha-numeric format. This would provide compatibility with older equipment and NOAA receivers while allowing for a

phase-in period. This method would not require costly hardware changes and reduce development time, thus resulting in lower costs and faster deployment.

## 7. ALERT VALIDATION

### e. Adding a Year Parameter to the "JJJHHMM" Timestamp

**Trilithic does not support adding a year parameter to the "JJJHHMM" timestamp. Instead, we propose better definition of the release time ("JJJHHMM") and valid time period ("TTTT") of the alert, which would require minimal changes to software and would not affect older EAS equipment or NOAA receivers.**

Within ¶141 of the NPRM, the FCC seeks comments on adding a year parameter to the "JJJHHMM" timestamp. Trilithic is not in favor of revising the rules to add a year parameter. This addition will require changes to the EAS Protocol header codes which affect the EAS equipment's FSK processing and potentially obsoletes older EAS equipment and NOAA receivers. For this reason we believe that the benefits do not outweigh the costs.

Past problems with the timestamp were largely due to clock drift in older EAS equipment. The accidental EAN in 2007 had a timestamp that was off by over two hours, raising concerns about the time accuracy for an actual EAN. EAS manufacturers compensated for this by allowing large time tolerances. Since the adoption of CAP, EAS equipment has access to network based timekeeping which has greatly improved accuracy. Tighter tolerances can now be implemented, making the window of time in which a recorded alert could activate an EAS Decoder very small.

Instead of changing the EAS header codes, rules can be adopted or more clearly defined about the release time ("JJHHMM") and valid time period ("TTTT") of the alert, which would require minimal changes to software and would not affect older EAS equipment or NOAA receivers. The rules could require that the release time be no more than 15 minutes in the future and the message must not be expired. This would reduce the margin of error to once a year for the valid time period of the alert.

For example, an alert that's encoded on Julian day 100 at 10:00AM with a time period of thirty minutes could only be accidentally retransmitted in following years if it is received on Julian day 100 between 9:45AM and 10:30AM. This would have, for instance, prevented the Bobby Bones EAN incident.

If the Commission does decide to add the year parameter, Trilithic recommends that it be placed at the end of the EAS header and limited to two characters in order to minimize the likelihood of adversely effecting older EAS equipment and NOAA receivers.

f. Validating the "LLLLLLLL" Station identification

**Trilithic supports the proposal to use the station identification ("LLLLLLLL") for validating alerts. It would have prevented as many of the cited false activations as any of the other proposed authentication or validation methods, while minimizing changes and costs.**

Within ¶142 of the NPRM, the FCC seeks comments on requiring the station ID ("LLLLLLLL") to be used for validating alerts. Trilithic agrees with this proposal and supports amending the rules to allow such validation. Software and configuration changes would be minimal, and costs would be limited to those associated with

testing and deploying new software. Validating the EAS header's station ID against the configured station ID's for the monitored sources would have prevented as many false activations as any other authentication or validation method proposed thus far.

g. Interstitial Alerts

**Trilithic recommends that interstitial alerts should never be considered valid alerts and should always be ignored.**

Paragraph 144 seeks comments on the handling of interstitial alerts. Currently Trilithic EAS Decoders ignore all interstitial alerts. Had this not been the case, the last national EAN test would have been interrupted. If an interstitial alert is detected, then it can be assumed that something has gone wrong with the original alert or the one that followed. Trilithic recommends that interstitial alerts should be ignored or cause the original alert to terminate (as if an EOM is received). They should never be considered valid alerts. Some conditions, such as EAS Decoders or radios in the background during a voice recording, could conceivably result in interstitial alerts even without equipment failure or misconfiguration.

**Alert Authentication and Validation Summary**

If authentication or validation rules are adopted which affect FSK processing, such as adding authentication data or a year parameter to the EAS Protocol header, then widely deployed legacy EAS equipment such as the EASyPLUS, EASyCAST, and EASyIP encoder/decoders that are still in use may not be able to be updated due to hardware dependencies of the FSK decoding process. Trilithic offers a next

generation EASyCAP Encoder/Decoder that can support any of the proposed rules through software updates. However, this will require more development cost and time than most previous rule changes. Conversely, the cost to develop and validate a change related to the station ID or strict time filtering would be minimal and would not result in any additional charges being passed on to our customers to offset the development of the new features.

## **8. REACH OF PROPOSED EAS SECURITY RULES**

### **a. EAN Only**

**Trilithic recommends that any new rules for authenticating and validating alerts should apply to all EAS events.**

Within ¶159 of the NPRM, the FCC seeks comments on implementing the proposed security measures for only the EAN or for all EAS alerts. Trilithic recommends that any new rules for authenticating and validating alerts should apply to all EAS events. The cost and complexity would be higher if new security measures only apply to the EAN. It would require more development and introduce a larger margin of error by having different operations occur depending on the event type. It would also increase the costs of long-term support, by requiring more maintenance and testing of the different operations for all software update going forward.

b. Exception for PN Stations

Within ¶160 of the NPRM, the FCC seeks comments on requiring a higher level of security for key EAS sources than for PN stations. Security breaches at key EAS sources could potentially affect a far larger section of the public than breaches at PN stations. Therefore, Trilithic believes that it makes more sense to require higher security measures for the key EAS sources as opposed to the PN stations. This could reduce the cost for implementing the proposed security provisions for most EAS Participants.

## 9. CENTRALIZED CONFIGURATION MANAGEMENT

**Trilithic strongly opposes the use of centralized configuration and management of EAS equipment due to security vulnerabilities, limited benefit, and high costs.**

Within ¶162-170 of the NPRM, the FCC seeks comments on centralized configuration and management for EAS equipment. Trilithic believes that first and foremost, implementing central configuration and management will increase vulnerabilities rather than improve security and reliability. It will require EAS equipment to provide management access on an Internet facing interface (presumably). EAS equipment is typically connected to an operator's management and video networks, and it's capable of overriding every channel in the system. Currently this equipment is protected from outside access. Requiring an interface for central management poses serious security risks to all of the EAS equipment in the country, introducing a single point of access that if breached could yield control to an attacker over every channel from every operator.

A centralized system will not improve distribution pathways, nor will it improve the geo-targeting of alerts, nor is it necessary to authenticate and verify alerts. State plans are responsible for defining EAS monitoring assignments, and consideration should be made to avoid single points of failure during the selection of those sources. If more granular targeting of alerts is desired, it should be accomplished by defining more granular location codes. This could be done using polygons for CAP messages and subdivisions for FIPS codes. If a centralized system to authenticate and verify alerts is desired, this can be accomplished more effectively by a system setup specifically for that purpose.

Automatically pushing the latest software to all EAS equipment is not workable, and would more likely cause problems and inconsistencies than provide more uniform and consistent operation. EAS equipment is responsible for interfacing with the equipment necessary to present audio and video alert information to the public, and this equipment varies greatly between systems. Software updates must be tested and vetted by individual operators to ensure compatibility and operation within their unique architectures before its deployed. The responsibility for testing and deploying any changes that affect a systems operations need to be left in the hands of those responsible for the system.

Implementing support for central configuration and management would require extensive modifications to EAS equipment's operations. It's unlikely that any legacy equipment would be able to support this. If adopted, Trilithic's EASyCAP Encoder/Decoder can accommodate these requirements with a software upgrade, but there will be a cost in order to fund the development effort.

## **10. NETWORK FUNCTION VIRTUALIZATION**

**Trilithic is not in favor of virtual EAS equipment because it would not provide any of the suggested benefits and would only burden EAS participants with additional costs and complexities.**

Within ¶¶171-174 of the NPRM, the FCC seeks comments on virtualizing EAS equipment or alert distribution. Trilithic is not in favor of virtual EAS equipment because it would not provide any of the suggested benefits and would only burden EAS participants with additional costs. Trilithic (and other) EAS equipment provide audio outputs and switches, video outputs and switches, MPEG outputs, control mechanisms for routing and distribution equipment, and interfaces for character generators, graphics systems, automation systems, and middleware. EAS equipment provides the content and controls the equipment necessary to present the alert audio and video to the public. These functions cannot be virtualized or put on cloud-based servers because hardware is needed at the operator's facility.

Furthermore, the small amount of operations that could be effectively virtualized would require an API that would likely be more problematic than the functions it seeks to replace, accomplishing little other than adding another layer of protocols and providing a more attractive, centralized target for attacks.

## **11. ENSURING A MODERN AND EFFECTIVE EAS STRUCTURE**

**Trilithic strongly supports the continued distribution of emergency alerts through both the broadcast-based EAS Protocol and IP-based CAP sources for redundancy and resiliency.**

Within ¶175-178 of the NPRM, the FCC seeks comments on how traditional broadcast-based EAP Protocol and newer Internet-based CAP-formatted IPAWS systems should relate to each other going forward. Trilithic strongly supports the continued distribution of emergency alerts through both the broadcast-based EAS Protocol and IP-based CAP sources for redundancy and resiliency. Broadcast and Internet distribution paths tend to be distinct from one another, providing separate vulnerabilities that enhance their effectiveness in regard to redundancy. In addition, CAP sources are still not utilized as often as traditional broadcast EAS sources for local weather and emergencies.

Traditional broadcast-based EAS has never been particularly secure; however there have been very few instances of malicious exploitations over the last twenty years. The only incident cited in this proceeding is the Zombie Attack Hoax, which was not due to EAS Protocol vulnerabilities, but rather a disregard for security when connecting EAS equipment to the Internet. Most of the incidents cited in this proceeding would not be prevented by the proposed ideas because the alerts were originated from legitimate EAS Encoder's, which would have inserted the appropriate security data and been indistinguishable from a valid alert.

A possible way to reduce the likelihood of similar accidents and exploitations would be to limit the alert origination capability of EAS participants that do not normally originate emergency messages.

## **12. COMPLIANCE TIMEFRAMES**

**Trilithic believes that any rules that change the EAS protocol FSK header codes will require at least a 24 month implementation period. Modifications that do**

**not affect the EAS Protocol FSK header codes would require a 12 month implementation period.**

Within ¶179 of the NPRM, the FCC seeks comments on the timeframes in which the proposals in this NPRM, if adopted, could reasonably be implemented by EAS participants. Any rules that change the EAS Protocol FSK header codes will require at least a 24 month implementation period. Legacy equipment will need to be replaced by some EAS participants. EAS Encoder/Decoder software will need to be revised, and once the updates are available operators will need 6-12 months for test and deployment. A 12 month implementation period should be sufficient if only station ID and/or strict time validation is required (and FSK processing is not affected) because modifications are minimal and can be made available shortly after rules are adopted, and it would not necessarily obsolete all legacy equipment.

Respectfully submitted,

/s/ Michael Maginity

Michael Maginity

Trilithic Incorporated  
9710 Park Davis Dr.  
Indianapolis, IN 46235  
(317) 895-3600

June 7, 2016