Before the
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

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

RE: COMMENTS OF MONROE ELECTRONICS IN REGARDS TO THE NOTICE OF PROPOSED RULEMAKING

1 Introduction

Monroe Electronics hereby respectfully submits the following comments and recommendations in response to the Public Safety and Homeland Security Bureau's Notice of Proposed Rulemaking.. We appreciate the great time and effort invested by the Commission in compiling this *Notice* . The *Notice* poses a great number of key questions on improving the Emergency Alert System that warrant serious consideration and debate across industry.

Monroe Electronics is strongly committed to the improvement of the national Emergency Alert System, including enhancing the security, reliability and functionality of the system. Monroe Electronics has been focused on the development and deployment of emergency alerting systems, and many broadcast and cable television operations rely on our solutions for their Emergency Alert System (EAS) and Common Alerting Protocol (CAP) operational requirements.

We appreciate the efforts of the Commission continue to examine the Part 11 rules governing EAS. While we share the same overarching interest as the Commission in these improvements in many areas, we detail some of our concerns below in the FCC's proposals, based on our experience in designing, building and supporting public warning systems for broadcasters, cable TV operations and public safety agencies across the nation. Our specific concerns, detailed below, raise the broader issue that several of the FCC's proposals and areas of inquiry may have unintended impacts on the nation's alert and warning systems, and may adversely impact several industry-wide developments already under way regarding advanced public warning capabilities.

For these reasons, we hope the Commission will duly consider our recommendations for the immediate rule changes it is contemplating, and will adopt our recommendation to utilize an industry forum of EAS stakeholders to consider more far ranging and long term enhancements to the nation's Emergency Alert System.

2 State EAS Plans are a critical resource for EAS Manufacturers and other EAS stakeholders; access to plans should not be withheld from those with a need for this information for essential EAS support and technical development functions.

At ¶ 30 (Security) in the *Notice*, the Commission seeks comment on whether access to State EAS Plan data should be limited and secured, as recommended by the Commission's Communications Security, Reliability Council (CSRIC IV), and on the steps it should take to safeguard against unauthorized access to SEPFI. While Monroe Electronics served on CSRIC, we did not necessarily support this particular recommendation in its final form.

Most information contained in, and pertaining to, State EAS plans are already a matter of public record, or readily discoverable. Further, the information contained in State EAS plans is needed by a variety of organizations to ensure both the efficient operation of the EAS, as well as the proper configuration of hardware and software within the EAS system. While we are supportive of the need to safeguard truly sensitive information, access to state EAS plan data is legitimately needed by a variety of direct and indirect stakeholders, including EAS equipment manufacturers and broadcast/EAS planning consultants. Monroe Electronics, for example has a legitimate and necessary need to regularly access state EAS plans for essential customer support and advisory functions for its many public safety, cable, IPTV and broadcast customers. Removing access to such state EAS plans would severely inhibit several basic customer support and system design functions provided by our company and others.

Certain information, such as internal state and local public safety agency activation procedures, may be considered sensitive information by these entities, specifically where such activation procedures identify individual personnel, equipment, software or services utilized for public safety and/or public warning communications. Information that may also be considered sensitive is the non-public contact information of specific individuals, such as telephone numbers, mobile phone numbers, email addresses and particularly afterhours/off-duty contact information of those involved in the actual activation of the EAS, including emergency operation center and public safety personnel, other government officials, and specific broadcast engineers at state relay, local primary and primary entry point stations.

An additional consideration we raise is the potential for any complication that may arise by the securing by a Federal organization of information, such as local agency operational procedures, that may otherwise have been considered in the domain of state, local, territorial or tribal government operations.

3 We support the electronic filing of state EAS plans; and note the need for sufficient flexibility in the on-line template to accommodate diverse state and local public warning architectures and use cases.

Our principal comment regarding the on-line filing of state EAS plans is that any on-line plan template should be sufficiently flexible encompass the diverse operational and technical requirements of the 50 states, plus territories. The template should be able to accommodate the broadest variety of dissemination architectures and local planning considerations, and to permit the incorporation of near-future technologies and approaches – such as alternative dissemination of CAP or FSK EAS alert messaging - which may be implemented in any state.

Regarding the question of whether the SEPFI template should be based on the Washington State EAS Plan documentation in CSRIC report, we observe that while the Washington State EAS plan is very comprehensive and methodical in its approach, it may be burdensome for some states that do not benefit from the same level of organization and activism that is enjoyed in the Washington State EAS community.

4 We support the re-establishment of a National Advisory Committee, but recommend that the NAC both be also fundamentally reconstituted with membership expanded reflect diverse stakeholders, including EAS equipment manufacturers, cable and IPTV providers, satellite service providers, and other Federal, state and local government agencies responsible for public warning.

At ¶ 32 (National Advisory Committee) in its *Notice*, the Commission raises the reestablishment of the NAC. Monroe Electronics support the idea of reestablishing the NAC. However, in addition to the named parties in the *Notice*, the NAC must include representatives from EAS manufacturers as system stakeholders, including the standards-setting functions of the EAS-CAP Industry Group (ECIG). In addition, the membership of a re-established NAC must include representatives from the cable and IPTV industries, including the National Cable Telecommunications Association and American Cable Association, as well as the various Federal and state agencies which utilize the EAS (including DHS FEMA and the National Weather Service).

Many of the proposals and questions posed by the FCC, particularly in regards to future architectures for the nation's EAS, deserve broad-based consideration by the full range of EAS stakeholders. The NAC could be a useful forum for such an activity, and should therefore also be reconstituted with a sufficient degree of independence to undertake the deliberations that may be required. We believe it is essential for a stakeholder forum to develop a consensus on whether an enhanced EAS architecture is needed, and if so, identify the most appropriate technological and operational options.

In this sense, the re-establishment of the NAC should follow the successful model of the Commercial Mobile Service Alert Advisory Committee (CMSAAC),

which brought together a broad range of industry stakeholders and attained a respectable degree of consensus around architecture and technical recommendations – recommendations which were by and large adopted by the Commission. The result of the CMSAAC process was the successful Wireless Emergency Alerts (WEA) system.

The Commission would be well served in following the CMSAAC model both in the re-establishment of the NAC, as well as using this re-established entity as the appropriate forum to provide input on future architectures and options for the nation's Emergency Alert System.

5 We support the proposed changes to 11.46, specifically to permit Public Service Announcements and commercially-sponsored announcements to explain the EAS to the public, provided that the entity using the codes and Attention Signal presents them in a non-misleading and technically harmless manner.

Firstly, we presume that the airing of Public Service Announcements would be strictly voluntary on the part of EAS Participants. EAS Participants should not be required by any party to place such Public Service Announcements on their air, though they may be encouraged to do so.

If EAS-like tones are included in such Public Service Announcements, such as but not limited to using some form of EAS codes and Attention Signal, we strongly suggest that that any replication of the codes should occur in a

frequency just outside those frequencies specified at §11.31(a)(1). All EAS encoder/decoders, if operating within specifications provided by the FCC, would not detect frequencies outside of those specified at specified in §11.31(a)(1).[1]

We further suggest that any replication of the codes should not utilize any actual or authorized SAME event code value. At a minimum the replication of an event code should not be one that is typically used for airing. In this regard, limiting such replication of codes to an RWT (required weekly test) event code may suffice in limited the potential for undesirable technical results. Likewise, we suggest that the codes should not utilize an actual FIPS code value, or alternatively should utilize a FIPS representing an area with no appreciable human population. If the actual EAS frequencies as specified at §11.31(a)(1) are utilized, the recommendation not to use actual SAME and/or FIPS codes is vitally important.

A sample or schema for technically harmless codes could be:

1. use of frequencies +/- 100Hz outside those specified at §11.31(a)(1);
2. with a non-valid ORG code of "*AAA*", a
3. with a non-valid event code of "*EEE*";
4. with a non-valid PSSCCC code of "*999999*".

---

[1] The Minnesota PSA referenced by the FCC included EAS tones that were intentionally modified to be outside the range specified in §11.31(a)(1); specifically the EAS tones were shifted approximately 100 - 150Hz, which was more than sufficient for the purpose of preventing any EAS equipment react or detect these EAS tones. As a result, these tones did not activate any FCC compliant EAS device, nor did these devices even log the presence of these tones.

5. with an LLLLLLLL value of "*EXAMPLE*" or some similar illustrative value

None of these values are currently in use for EAS, and could be reserved as a schema for any demonstration or illustrative purposes, such as inclusion in a PSA. These values in the EAS header would be composed as follows, and would be technically harmless as far as processing by EAS encoder/decoders:

ZCZC-AAA-EEE-999999+TTTT-JJJHHMM-EXAMPLE

We also suggest that any codes or attention signal should be used at a volume level below that of the average audio level of the PSA. This, in our opinion, would be of assistance in keeping the included alert tones in the context of a simulation, or in the background, compared to the full audio volume level that should be reserved for an actual EAS alert.

6 While we support the development of an IP-first approach to EAS, the FSK-based EAS relay has shown itself to be an indispensable part of a robust national public warning capability. We strongly recommend that the FSK-based EAS must remain both as a complementary alerting path and an essential backup in the event of the unavailability of IP networks during an emergency.

Hurricane Sandy provides a poignant example of the impact of severe weather on the resiliency of Internet-based systems. This major storm event caused major power and Internet outages in a region of more than 60 million people. The impacts on Internet connectivity were severe, not only in NYC, Long Island, and New Jersey, but also peripheral weather-related outages as far south as the

Washington DC area, and up the I-93 corridor from Boston into New Hampshire.[2]

With conventional Internet disrupted in these areas, the ability to monitor CAP-based alerts was greatly impacted.[3] At the same time, anecdotal information we received at the time from the impacted area indicate that the broadcast EAS relay was not substantially impacted during this major storm event.

The FSK-based EAS relay is a key part of the national PEP alert relay capability, upon which the dissemination of Presidential messaging (the EAN) is primarily based. Importantly, there is nothing on the record indicating that FEMA/WHCA intends to eliminate use of the PEP system, even if it does in part use CAP. In fact, everything we have been told and have independently observed about the PEP relay system indicates that it will relay a key component of a resilient and survivable national warning strategy for years to come. The EAS system, in our assessment, remains essential capability to ensure that national authorities can under all conditions provide alerts and warning to the American people, whether that role is as a primary system (PEP),

---

[2] Dout Madorie, Dyn Research, "Hurricane Sandy: Initial Impact," http://research.dyn.com/2012/10/hurricane-sandy-initial-impact/; Jim Cowie, Dyne Research, "Hurricane Sandy: Outage Animation," http://research.dyn.com/2012/10/hurricane-sandy-outage-animati/; Jack Clark, "Hurricane Sandy doubled failures in US internet infrastructure," December 19, 2012, http://www.zdnet.com/article/hurricane-sandy-doubled-failures-in-us-internet-infrastructure/; Marguerite Reardon, "Hurricane Sandy disrupts wireless and Internet services," October 30, 2012, http://www.cnet.com/news/hurricane-sandy-disrupts-wireless-and-internet-services/.

[3] Additional public warning issues surrounding this event are discussed in Carl Weinschenk, "Hurricane Sandy and EAS-CAP," Broadband Technology Report, November 21, 2012. http://www.btreport.net/articles/2012/11/hurricane-sandy-and-eas-cap.html

redundancy/back-up, or survivable messaging path in a post-event and/or transitional environment.[4]

For these reasons, we answer with a resounding "yes" to the question of whether the Commission should maintain a secondary broadcast EAS system based on legacy EAS in addition to the IPAWS-OPEN based system. Elimination of the EAS relay will pose knowable risks and dangers far in excess of any potential perceived benefits. Maintaining the EAS relay will provide a critical backup capability to the IPAWS-OPEN based CAP system.

As detailed in our previous proposals on enhancing the broadcast EAS (including use of the Textual Data Exchange method to include additional data in the EAS message), and our current proposal to implement an "immediate polling" capability upon receipt of EAS messages (described in section 7 below), the legacy EAS can be more closely synchronized with the IPAWS-OPEN-based system, such that the maintenance of a legacy EAS should not be viewed as something "separate from" IPAWS OPEN. The EAS relay should be viewed as complimentary to - and something that can be further integrated with - the CAP-based system as a resilient secondary path and backup.

---

[4] Executive Order 13407 - Public Alert and Warning System (June 26,2006) specifies that two of the functions of the Secretary of Homeland security are to "administer the Emergency Alert System (EAS) as a critical component of the public alert and warning system"; and to "ensure that under all conditions the President of the United States can alert and warn the American people." (https://www.gpo.gov/fdsys/pkg/WCPD-2006-07-03/pdf/WCPD-2006-07-03-Pg1226.pdf)

7 To further synchronize and integrate the broadcast EAS system with the IP-based CAP system, we propose the addition of a feature to EAS equipment that would allow such equipment to immediately poll a source for a CAP message upon receipt of an FSK-based EAS message.

We support an evolution towards an "IP-first" environment, which can utilize more informative CAP messaging and associated resources. However, we do not support an "IP-only" environment, which – as discussed below – would remove the critical fallback role of the broadcast EAS system. We feel this would be an unwise choice.

The benefits of CAP messaging are clearly evident: more in-depth information, support for multilingual messaging, ability to support multimedia resources. However, for various reasons, a broadcast EAS message may be received by an EAS participant before a CAP message. Further, it is not clear that CAP-based messaging alone represents a fully resilient and survivable public warning capability under all conditions, as evidenced in our references to the impacts of Hurricane Sandy above. Such disruptions are not entirely uncommon, as again in the case of the progressive derecho of June 2012, which tracked across a large section of the Midwestern United States and into the mid-Atlantic states. This storm event resulted in widespread damage and millions of power outages across the entire affected region.[5]

---

[5] "Impact of the June 2012 Derecho on Communications Networks and Services". Public Safety and Homeland Security Bureau, Federal Communications Commission, January 2013, http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0110/DOC-318331A1.pdf; "Maryland Public Service Commission, After Action Review, June 29, 2012

Even under presumably normal circumstances, we have identified numerous cases where an FSK-based EAS message is received before a CAP alert message. This can be due to numerous reasons, such as the polling interval of CAP EAS equipment, network issues at the EAS Participant, or issues at the EAS Participant's ISP.

To ground these concerns, the result of the first CAP RMT test in the state of Minnesota during November 2013 provides useful data.[6] In this test, an RMT was simultaneously issued in both CAP XML and broadcast FSK EAS formats. A report from the Minnesota Division of Homeland Security and Emergency Management indicates that 75% of respondents received the CAP message first, and transmitted it accordingly. However, 21% of EAS Participants responding the survey received the broadcast EAS message, rather than the CAP message. Of these 1/3 received the broadcast EAS message first, while 2/3 reported not receiving a CAP message at all. A further 4% received no RMT message from either CAP or broadcast EAS.

From the example above, it is clear that 21% of EAS Participants were able to air an alert message because the conventional broadcast EAS played a critical role as a backup to the CAP system. We do not think that the experience of this

---

Derecho Storm Event," Maryland Public Service Commission; "D.C. storm 2012: Power out for thousands, damage reported throughout D.C. area," WJLA, 30 June 2012, http://www.wjla.com/articles/2012/06/d-c-maryland-virginia-power-outages-and-road-blockages-77457.html;

[6] "Report on the Common Alert Protocol (CAP) generated Required Monthly Test (RMT) of the Emergency Alert System, 6 November 2013," prepared by the Minnesota Department of Public Safety, Division of Homeland Security and Emergency Management.

state is atypical, and demonstrates the continued utility of the broadcast EAS message as a critical redundancy to the CAP based system.

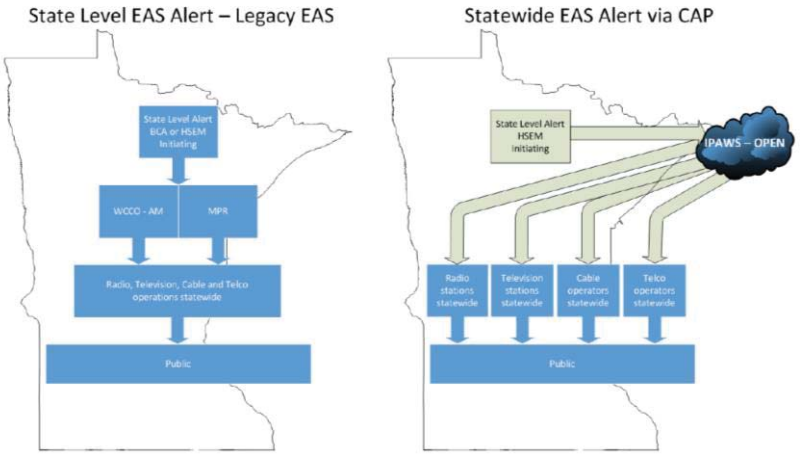

Figure 1: Example of Complementary EAS dissemination paths (Minnesota CAP/EAS RMT - November 2013)[7]

To better balance situations where a broadcast EAS message is received before a potentially more informative CAP message, we propose a mechanism by which the EAS equipment would immediately poll the CAP source (IPAWS) upon receipt of any FSK-based EAS message.

- If a broadcast message is received, the EAS equipment would immediately poll IPAWS. If the EAS equipment identifies an identical corresponding

[7] Ibid.

CAP message, then the EAS equipment should utilize the CAP message, which is presumably more informative than the broadcast EAS message.

- However, if the EAS equipment does not find a CAP message that corresponds to the FSK message, then the EAS equipment should proceed with the received FSK EAS message.
- Both CAP and FSK EAS messaging contain parameters that are used for duplicate detection and filtering (that is, CAP message parameters are mapped to EAS header parameters. If these parameters are identical, then the EAS equipment would normally treat the second message as a duplicate, and ignore it.

With our proposed methodology, the EAS equipment would actively seek the CAP source and relay the CAP message instead of the EAS message, giving preference to the presumably more informative CAP message. The time to perform this function should be minimal (within 1-2 seconds after receipt of an FSK EAS message, usually within 1 second). The benefits may be significant, including the dissemination of more complete, informative and accessible public warning messages.

The automated workflow of this immediate polling process is illustrated in Figure 2 below:

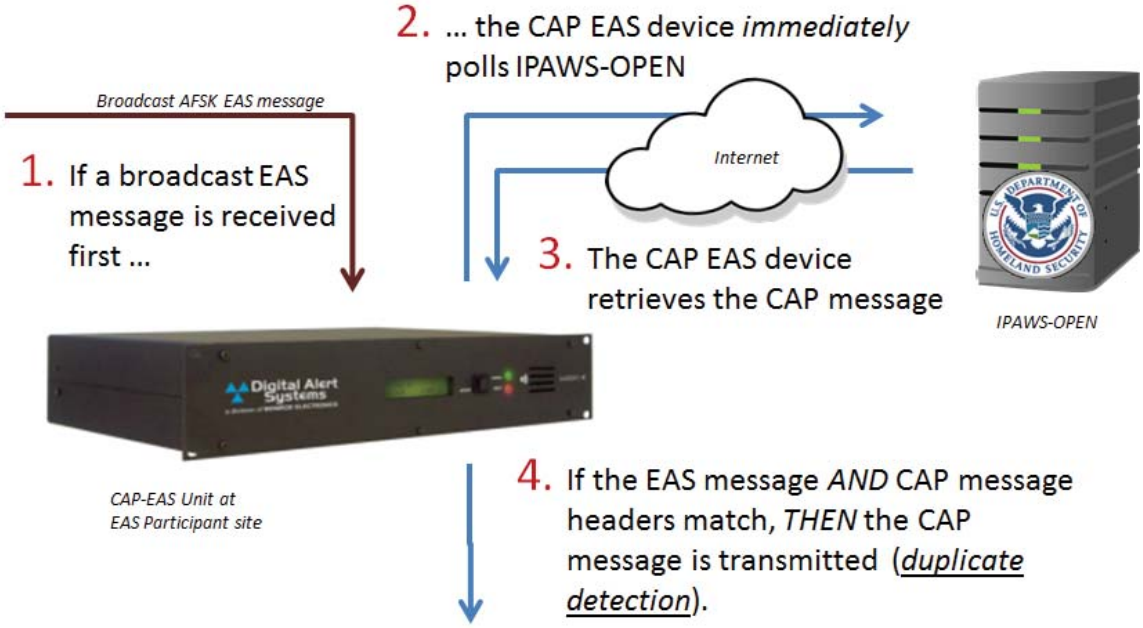

Figure 2: Immediate CAP message polling, if EAS message is received first.

The exceptions to this methodology may be the EAN and NPT event codes, due to the Commission's rules specifying that these alerts must be transmitted immediately upon receipt. However, even in these two defined cases, it may be argued that the one to two seconds that may be required to additionally poll the IPAWS OPEN system may be sufficiently limited and necessary as to fall within the Commission's intent of "immediate" transmission of these alerts.

8 The question of "lockouts" in the cable/IPTV industry, as described in this *Notice*, is incorrectly linked to the operation of EAS equipment.

In ¶ 132 of its *Notice*, the Commission seeks comment on a proposed rule to require all EAS Participants to report instances when their EAS equipment causes, contributes to, or participates in a "lockout" that adversely affects the public (e.g., when multiple cable STBs cannot return to normal operation due to the failure to receive an EOM signal or otherwise correctly process an EAS alert). We are concerned that the Commission may not be fully aware of the fact that such "lockouts" are not caused by EAS equipment, per se.

The phrasing of the Commissions' question is important, as it infers a specific causality (the output of the EAS equipment). The correct output of EAS equipment is not the cause of the "lockout" instances about which the Commission is seeking information. The properly formatted valid output from the EAS device should not cause a "lockout." In this sense, the presence of EAS equipment is merely incidental to the "lockout," unless one tenuously argues that the mere forwarding of a properly formatted alert "contributes to" or "participates in" a lockout.

Further, there is no recorded instance of EAS equipment (or specifically EAS equipment furnished by Monroe Electronics) causing any "lockout". More specifically, there has been no incidence that we are aware of relating to Monroe Electronics' equipment when any cable STB did not return to normal operation due to the failure to receive an EOM signal.

As such the question posted at paragraph 132 in the *Notice* may be based on an incorrect premise, and may likely as a result generate insufficient and/or incorrect information for the Commission. We therefore urge the Commission to

clarify or withdraw the proposed rule change at §11.45(b)(2) which would require "an initial report within 15 minutes of discovering that EAS Participant equipment causes, contributes to, or participates in a lockout that adversely affects the public. The report shall include the time discovered, message source, and affected devices."

9 The need for additional security and authentication in EAS messages can be supported by utilization of an ancillary protocol such as Textual Data Exchange (TDX), and an amendment of the EAS protocol itself may not be necessary. Most EAS equipment can support such changes by software/firmware update.

At ¶ 134, the Commission raises the need for the EAS protocol to include a method to ensure that an alert received by EAS equipment was originated by an authenticated source. Because the broadcast FSK-based EAS currently benefits from little internal security, it may be vulnerable from a variety of attack vectors, such as side-channel attacks and spoofing. Because the EAS protocol is itself a matter of public record, and because message examples are abundantly available in the public domain, the information in the EAS header could in principal be reused, recompiled or mimicked to exploit the system with a moderate level of technical knowledge.

We have proposed the inclusion of additional security and authentication elements within EAS messages, including a digital certificate algorithm for authentication, a unique message ID (which may coordinate with a companion XML CAP message), and a year parameter (YYYY as suggested by the Commission). We have suggested that this information can be transmitted and utilized via the Textual Data Exchange (TDX) methodology, which is an efficient

means of inserting this critical data into the EAS message, without altering or disrupting the EAS header.

TDX is a technique developed by Monroe Electronics for including additional text/data within a standard EAS audio transmission. TDX is an encoding schema that is spectrally more efficient than the AFSK used for the EAS header. It is a separate encoding schema that remains within the frequency range specified in the Commission's rules for EAS. TDX was originally presented to the FCC in 2004.[8] Several field trials since then have proven the protocol's interoperability.

At present the TDX technique is under evaluation by the FEMA IPAWS laboratory, as to its potential to address several issues raised by the Commission in its *Notice*. For this reason, we would strongly urge the Commission to defer any rulemaking or decision on addition of security and authentication parameters, including the proposed YYYY year timestamp, until and unless a technical authority such as the FEMA IPAWS laboratory has concluded their evaluation.

The TDX data packet can contain text, data and/or pointer information (e.g. hypertext), such as:

- A unique message ID for message authentication and deconfliction
- Information such as the YYYY parameter

[8] TDX was initially presented to the Commission by Digital Alert Systems in 2004. Please see ex parte of 22 October 2007 (http://apps.fcc.gov/ecfs/document/view?id=6519744155) and comments of Digital Alert Systems, 18 October 2004 (http://apps.fcc.gov/ecfs/document/view?id=6516743468).

- A digital certificate for message authentication
- CAP message <description> and <information> parameters
- A language tag
- Other specialized text or authenticators

TDX was designed to conform to FCC Part 11 rules, and does not modify existing EAS header or EOM data. TDX places a data packet within the audio envelope of the current EAS protocol. Again, TDX does NOT change the EAS protocol. Adoption would not obsolete the installed base of existing EAS equipment. Importantly, it would not interfere with the operations of NOAA/SAME weather receivers.

The TDX packet contains event specific data and/or pointer (e.g. hypertext) information directing decoder sites to event related data in an associated emergency database. The TDX packet can be placed before, during, or after any associated audio message. Duration is typically very short, but varies depending on the amount of data conveyed (some of the elements we have suggested may be transmitted in under 0.27 seconds).

The FEMA IPAWS lab has been provided with the TDX capability, to provide an independent, objective assessment of how the technique may resolve several key shortcomings of conventional EAS messaging. We urge the Commission to refrain from taking any decision regarding adding security and authentication to EAS messages, until and unless evaluation of TDX and/or other approaches are completed by an authority such as the FEMA IPAWS laboratory.

10 All CAP messages intended for EAS must include a digital signature, and must pass digital signature inspection. Further, we recommend that all FSK-based EAS messages must include a digital signature, and likewise pass digital certificate inspection.

We strongly support the position of the Commission that CAP alert messages must complete digital signature verification, using the digital credentials provided to alert originators from the FEMA IPAWS program. Digital signatures are widely recognized as a best practice for providing digital verification of electronic transactions, and provide "non-repudiation" — the ability to identify the author and whether the CAP alert message has been changed since it was digitally signed. Both the DASDEC and One-Net CAP/EAS emergency message platforms *currently* provide a means to require all CAP messages to pass digital signature inspection (that is, to remove the ability to process a CAP alert message that fails digital signature inspection).

Further, we recommend that FSK-based EAS messages should contain a digital signature algorithm, and be required to pass digital certificate inspection in a similar manner to the CAP XML message. Our discussion above proposes including this digital certificate within the TDX packet, so as to not interfere with the EAS headers.

The potential positioning of the digital certificate as part of the TDX envelope is illustrated in Figure 3 below:

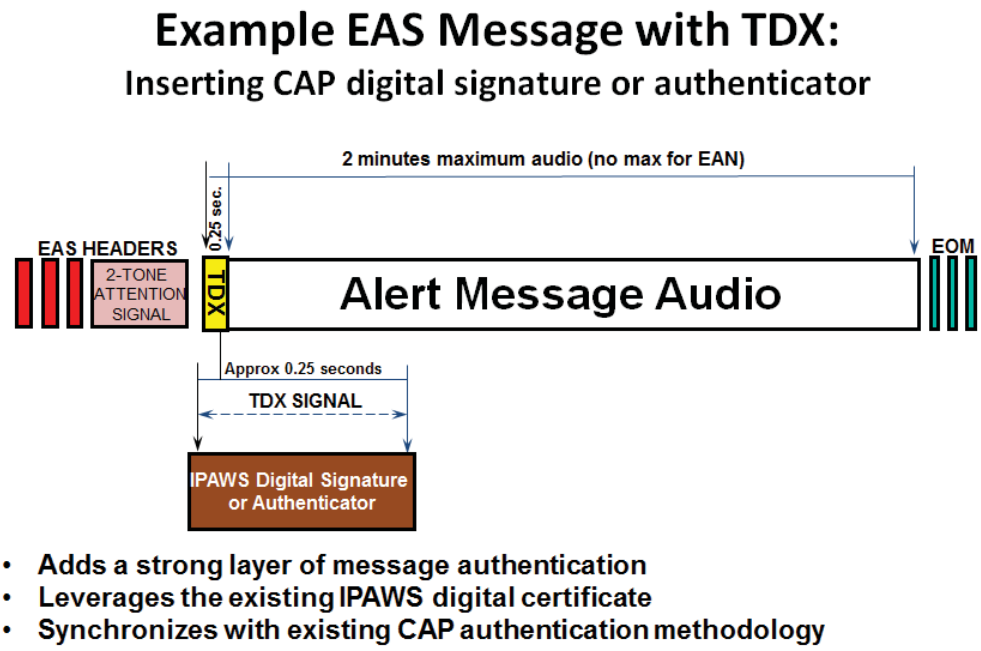

Figure 3: Example EAS Message with TDX: Including authentication info

11 The proposed change of § 11.33(10) to mandate use of the Station ID parameter for authentication purposes may prove to be of limited utility . Additional technical study is required to determine if this proposal would yield the results desired by the Commission.

We are generally very supportive of enhancing the authentication and security capabilities of the EAS protocol. However, we believe the specific proposal to utilize the LLLLLLL Station ID parameter deserves additional discussion, study and technical testing before any decision is made. The Commission proposes that a "header code must only be considered valid when two of the three headers match exactly, the Station ID header code matches one of the assigned

monitoring sources as specified in the state plan and the expiration time is in the future."

While EAS equipment could likely be modified by software update to utilize this Station ID parameter for validation, we are concerned that the Station ID parameter itself may not be appropriate for the objective of message authentication.

As an additional consideration, the proposed rule change to §11.31(c) change, specifies that the LLLLLLL would correspond to the PSID information of the EAS Participant. However, PSID identifiers are mainly used by cable and IPTV operators, while broadcast EAS Participants use facility IDs. State, county, local, territorial and tribal authorities likewise do not have PSID identifiers, and tend to set their own values in that parameter. However, both the PSID and Facility ID information is readily available in FCC public databases.

If this proposal is adopted, which we do not support, this LLLLLLL parameter should be validated in both the EAS and CAP message formats, for consistency.

CAP/EAS devices would need to add a LLLLLLL as a filter setting in their software, which would not be a trivial function given the potential number of Station ID values and monitoring assignments. The list of values to be populated in the Station ID parameter must be known, and any authorized changes to that value – no matter how minor or trivial – must be reported immediately, so users of CAP/EAS devices can manually update their filter settings, or if necessary manufacturers of CAP/EAS devices can provide periodic software updates with that changed information. Additionally, any change to monitoring assignments would consequently change the expected LLLLLLL value, requiring all EAS participants that monitor that changed assignment to

change, would result in a require filter settings change the monitoring EAS/CAP equipment. Such changes would need to be made uniformly, and in a timely manner, to ensure that valid EAS messages are not inadvertently rejected because the changed Station ID information is no longer valid.

There are a variety of other potential operational and technical factors involved in the implementation of this proposal, and for this reason we strongly suggest that the Commission reconsider this proposed rule change, At a minimum, any such decision be taken only after additional industry test and evaluation, including input from an independent assessment by the FEMA IPAWS laboratory.

12 The specific proposed changes in sections §11.31(c) and §11.32(5) of the Commission's EAS rules to include a year parameter "YYYY" in the time stamp may cause significant operational problems to key public warning systems and consumer public safety products.

The Commission has proposed to modify the EAS header to include a year in the time stamp by changing the JJJHHMM EAS header element to become YYYYJJJHHMM, with YYYY representing the year of message origination. We agree that the inclusion of a year data points would resolve a critical omission in the EAS header. However, the specific proposal, described below, will have several negative impacts, and should not be adopted in its current form. Rather, we propose that the YYYY time stamp either be relocated to the end of the EAS header, or preferably be utilized within the TDX protocol. In either scenario, additional testing by both manufacturers and independent resources (such as the FEMA IPAWS lab) would be highly advisable before adoption of any such change.

Under the Commission's current proposal to change the JJJHHMM header element, the existing EAS header, as depicted below:

ZCZC-ORG-EEE-PSSCCC+TTTT-**JJJHHMM**-LLLLLLLL

Would be altered to be formatted as follows:

ZCZC-ORG-EEE-PSSCCC+TTTT-**YYYYJJJHHMM**-LLLLLLLL

However, the particular method proposed by the Commission would very likely result in numerous unintended and undesirable outcomes.

Our understanding is that this proposed change to the EAS header may also have the unintended consequence of interfering with both National Weather Service operations, and interfere with the functioning of the many hundreds of thousands of NOAA weather radios currently used in homes, schools, shelters and other public facilities. That is, the appearance of the YYYY data element within the existing EAS schema may render the EAS header into something that would be seen as an "error" by encoding (NWS) and decoding (NOAA weather radios) equipment that utilizes the existing EAS header.

A modification of the FCC's proposed change could consist of inserting the YYYY parameter *after* the current EAS header string:

ZCZC-ORG-EEE-PSSCCC+TTTT-**JJJHHMM**-LLLLLLLL

Could be amended as follows:

ZCZC-ORG-EEE-PSSCCC+TTTT-JJJHHMM-LLLLLLLL-**YYYY**

It is possible that this latter formulation may not adversely impact NOAA Weather Radios, however we must defer to the National Weather Service to

comment on whether their systems could be modified to accommodate a revised EAS header string, in either scenario. In any event, we stress that considerable testing and evaluation must be performed to fully ascertain the impacts and necessary mitigations to accommodate the FCC's proposed changes. As a separate proposal, below we detail how the TDX protocol, as previously proposed to the FCC, could accommodate the desired outcomes of the new YYYY data point, without unnecessarily causing the potentially significant disruptions indicated above.

While the FCC's proposal could be accommodated in a software update provided by EAS manufacturers, this change would of course pose a major challenge for any equipment that is not currently supported (for whatever reason), or is not updated by the user. If any particular EAS Participant's EAS device is not updated in a timely manner after the release of such an update, that EAS device would likely not be able to properly process any received EAS message using the amended YYYYJJJHHMM time stamp. Of course, any EAS device that is no longer supported by a manufacturer would likewise no be able to properly process any received EAS message with this YYYYJJHHMM time stamp, and would in all likelihood need to be replaced.

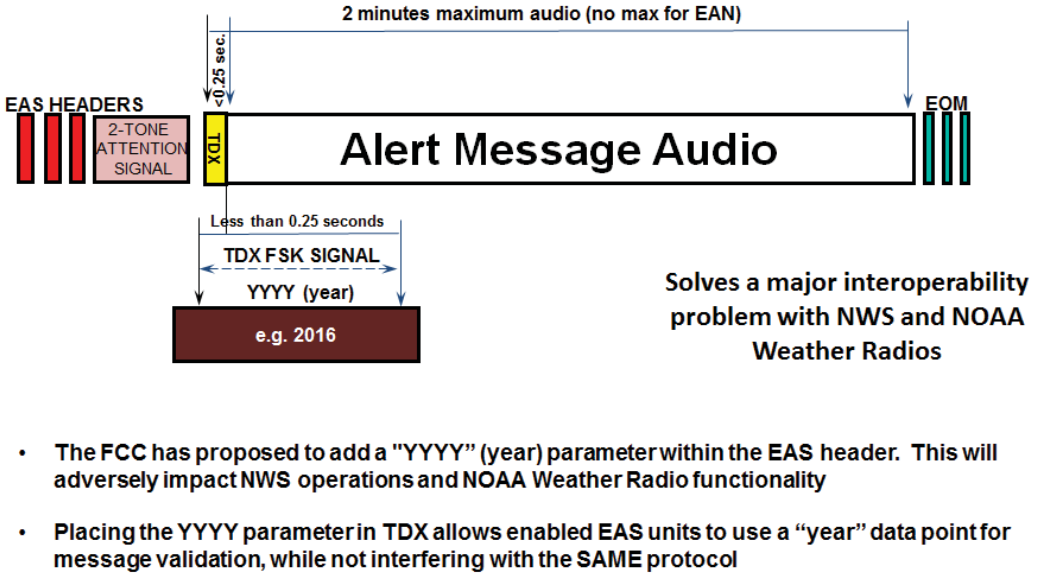

Figure 4: Example EAS Message with TDX: Incorporating the YYYY date parameter

For the obvious implications on public safety, we urge the Commission to either (a) defer any decision on amending the EAS protocol in this specific manner until further study is made, or (b) authorize the inclusion of the YYYY parameter in a TDX data packet, as illustrated above. The TDX approach is currently under initial evaluation by the FEMA IPAWS laboratory.

13 Instead, we suggest including a digital certificate algorithm, YYYY year parameter, and possibly a unique message ID as part of a TDX packet.

At ¶ 137, the Commission cites our TDX protocol that can add a cryptographic digital certificate, unique message ID, and or year (YYYY) parameter. This is

not an analog version of the CAP digital signature, rather this is the encapsulation of the same CAP digital signature in an FSK EAS message.[9] Any such solution should have the benefit of impartial testing by a resource such as the FEMA IPAWS laboratory.

We state to the Commission that Monroe Electronics would intend to make the TDX protocol available without compensation, upon request to any and all FCC-certified EAS manufacturers for the purpose of implementing the protocol for the purposes of the Emergency Alert System.

TDX can enable analog EAS messages to benefit from the same level of authentication afforded to CAP messages with digital signatures can provide authentication for messages propagated via IPAWS-OPEN or other IP-based systems. We amend some of our earlier suggestions[10] , to note that:

1. Including a digital signature would significantly improve message security with usage of this authenticator.
2. Including of a unique message ID, a data element favored by the National Weather Service, could also be transported via TDX. This unique message ID could also last a fraction of one second.
3. Including the YYYY date code in TDX would also enhance message security, while avoiding the potential disruptions of revising the SAME

---

[9] We offer a clarification to the Commission regarding TDX capability. Contrary to the Commissions statement in the *Notice* that TDX uses FSK tones, TDX is a separate encoding schema, that remains within the frequency range specified in the Commission's rules for EAS.

[10] See *Monroe* Comments at 5.

EAS header. Again, the YYYY date code would last a fraction of one second.

4. Transmission of all three new elements – digital signature, unique message ID and YYYY date code – would result in enormous improvements to EAS message security, and add a data burst of approximately 1 second to 1.25 seconds. This is substantially less than the 2-4 seconds initially suggested in our previous filing.

14 TDX would both support and enable a version of the Virtual Red Envelope concept proposed by the Broadcast Warning Working Group.

In addition, we note that the TDX method of adding analog authentication mechanisms is not only compatible with the Virtual Red Envelope concept, we find that TDX can be the actual operational implementation of the "Virtual Red Envelope" (VRE) proposal offered by the Broadcast Warning Working Group.[11] The VRE proposal generally suggests that that CAP EAS equipment should receive an authentication mechanism to validate broadcast EAS messages. Another way of viewing the VRE proposal is that it would incorporate any standard authentication mechanism in the EAS message, such as a digital credential, or "lock and key" approach.

Both our TDX and the BWWG's VRE proposals are complimentary, in that they essentially support the use of an analog version of the CAP digital signature to confirm the authenticity of EAS messages originated in the EAS Protocol. To

[11] The BWWG proposal can be found at Comments of the Broadcast Warning Working Group (BWWG), PS Docket 14-200, http://apps.fcc.gov/ecfs/document/view?id=60000989758.

confirm the authenticity of received broadcast EAS alerts, we have proposed adding a digital certificate algorithm, a unique message ID or other authenticator after the existing EAS header codes, as part of the TDX packet.

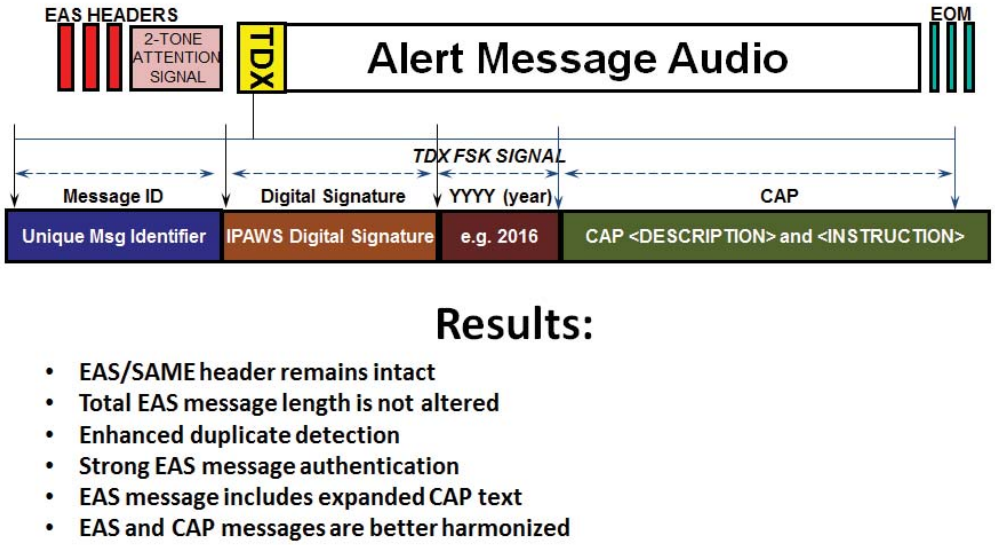

Figure 5: Example EAS Message with TDX: Incorporating the IPAWS digital signature, YYYY timestamp, unique message ID, and CAP alert text.

As an example, the TDX solution provides an analog version of the CAP digital signature to be decoded downstream. We concur with the FCC's assessment that if such an analog version of a digital signature had been in use during the Bobby Bones Show Incident, Zombie Attack Hoax, or the ARCO/BP Advertisement Incident, or any other incident where live code alerts were mistakenly sent during test events, EAS equipment would have treated the unauthorized alert as inauthentic because they lacked a valid signature (or lacked a signature at all).

The benefits of implementing TDX across industry vastly outweigh any potential development or software update costs that may be involved in improving EAS equipment with this capability. As note, to further mitigate the costs of such a valuable improvement to the nation's EAS, Monroe Electronics is prepared to provide the specifications to TDX to all FCC-certified EAS manufacturers upon request, with no compensation. The TDX packet, depending on its content, can be relatively unobtrusive and may result in the inclusion of additional data tones of only 0.27 to 1.25 seconds in duration for key authentication information. The benefit, in our opinion, would be a much more secure and robust EAS capability with no loss of functionality while older non-TDX systems are replaced.

15 Modern CAP EAS equipment performs complex and integrated functions within the embedded plant EAS Participant's architectures. This and other considerations warrant consideration by all stakeholders in a forum, as the most effective venue for the examination of future EAS architectures.

Today's CAP/EAS devices are much more than a simple receiver and audio switch. Modern CAP/EAS devices perform an increasingly broad range of functions that are tightly integrated into core operating functions at broadcast, cable and IPTV operations. To help the Commission understand the role of certain types of CAP EAS equipment in today's broadcast, cable TV and IPTV plants, we provide the following overview.

The predecessor to EAS was the Emergency Broadcast System (EBS), which featured receivers that were little more than a simple decoder triggering an audio switch, with limited functionality. In the 1990s, these rudimentary devices were replaced by a first generation of EAS encoder/decoders capable of

decoding EAS tones, encoding EAS tones, perform basic audio switching, and provide serial textual output (in a very limited number of formats).

However, a next generation of EAS product device emerged, going far beyond the limited functionality of conventional EAS encoder/decoders. These more fully featured emergency message platforms – at least in the case of our DASDEC™ and One-Net™ - fulfill the additional roles of an emergency content management server, message router, transcoder, video encoder, and a great deal more. These fully featured EAS devices appeared well before the adoption of CAP, though CAP impelled a broader range of interoperable features.[12]

Without disclosing confidential or proprietary functions of the DASDEC and One-Net CAP/EAS equipment, we advise the Commission that this equipment not only is responsible for encoding and decoding of EAS messaging, but is integral to the core function of EAS message composition and display. Below are a few of the integrated functions of the DASDEC and One-Net systems:

- Monitors inbound digital channels, with onboard software, whether Internet, VSAT, DVB, or ATSC IP broadcast.
- Reformats and transcodes received EAS messaging into CAP, for use downstream.
- Transcodes EAS messaging into any of over 50 digital (IP based) formats, and over 70 serial based formats used to communicate with downstream systems. Many of these formats are proprietary to middleware and

[12] The DASDEC provided support for the Common Alerting Protocol as early as 2004, a decade before formal FCC adoption of the CAP messaging standard in its rules.

downstream system vendors. A number of key formats are proprietary to the EAS manufacturer.

- Aggregates, routes and manages emergency message traffic within complex architectures
- Creates visual EAS displays via an onboard character generator
- Encodes EAS video, including into MPEG streams, for display to the consumer
- Transcodes EAS messaging into over a dozen different languages, with both textual and text-to-speech support.
- Provides onboard storage for years of EAS events, including full audio and multimedia captures, for compliance and playback purposes.
- Internal control, alert aggregation, log collection and monitoring of remote EAS equipment (within the enterprise).

As evidenced in the above description above the DASDEC's functionality represents a key asset in broadcast and cable system plant that fulfills a variety of roles that would otherwise require potentially a dozen or more separate components, at significantly (and exponentially) higher cost than that of the EAS/CAP equipment alone.

The actual insertion of emergency alerts into broadcast and cable environments in many cases requires a physical presence, including physical interfaces, that is provided by physical EAS equipment. Further, whether in broadcast TV, cable TV or IPTV, the successful functioning of the alert interrupt in the programming stream is managed by software and messaging protocols that are in many cases controlled by the EAS/CAP device.

16 In several key areas, our EAS equipment is deeply integrated with advanced technology deployments in broadcast and cable plant, and is a core enabling technology.

Modern EAS equipment not only supplies a variety of operational functions for EAS Participants, and particularly in the case of Monroe Electronics' solutions, this equipment is deeply embedded in the workflow and infrastructure of broadcast and cable operations.[13]

In significant areas, Monroe Electronics has helped foster innovation, and are enabling future development, in both the digital television and cable/IPTV industries. Monroe Electronics, for example, has been a key innovator in such areas as CAP/EAS systems for public safety agencies[14], multilingual alerting[15],

---

[13] A few examples of the integration of CAP EAS equipment and broadcast/cable plant are cited at: Michael Balderston, "*DAS and BroadStream Partner on EAS Messaging Playout: DASDEC EAS and CAP platforms integrated into Oasys*," TV Technology, 14 April 2016. http://www.tvtechnology.com/equipment/0005/das-and-broadstream-partner-on-eas-messaging-playout/278463; "*Digital Alert Systems and Hardata Partner to Reduce Cost and Complexity of EAS Compliance: Integration of Company's DASDEC EAS Platform With Hardata Video Server Line Simplifies Playout of EAS Messages Over Multiple Channels*," Multichannel News, 5 December 2014. http://www.multichannel.com/prfeed/digital-alert-systems-and-hardata-partner-reduce-cost-and-complexity-eas-compliance/386075; "*Blonder Tongue, Monroe Electronics Collaborate on Emergency Alert Management Solution*," Government Video, 5 February 2014. http://www.governmentvideo.com/article/blonder-tongue-monroe-electronics-collaborate-on-emergency-alert-management-solution--/114962.

[14] One example of public safety usage is referenced at "Texas Department of Public Safety Installs Digital Alert Systems Equipment to Handle Statewide Emergency Alerts," Government Video, May 7, 2014, http://www.governmentvideo.com/article/texas-department-of-public-safety-installs-digital-alert-systems-equipment-to-handle-statewide-emergency-alerts/115086; "Texas DPS Installs Digital Alert Systems Equipment To Handle Statewide Emergency Alerts," Homeland Security Today, May 7, 2014, http://www.hstoday.us/briefings/industry-news/single-article/texas-dps-installs-digital-alert-

alternative IP relay of alerts including ATSC-based data broadcasting[16], Mobile EAS (MEAS)[17], and next generation digital television alerting standards such as ATSC 3.0.[18]

---

systems-equipment-to-handle-statewide-emergency-alerts/3fd9162b9198cb183d39174128c7faae.html.

[15] "Multilingual EAS Test in Minnesota Tests Broadcasting," RadioWorld, April 14, 2015, http://www.radioworld.com/article/multilingual-eas-test-in-minnesota-tests-broadcasting/275603; "Rick Wimberly, "Multilingual Alerts Tested," Emergency Management, November 22, 2015, http://www.emergencymgmt.com/emergency-blogs/alerts/multilingual-alerts-tested.html; Susan Ashworth, "IPAWS Completes First Bilingual EAS Test," RadioWorld, November 18, 2015, http://www.radioworld.com/article/ipaws-completes-first-bilingual-eas-test/; "Bilingual Emergency Alert Gets First Test," Inside Radio, November 20, 2015, http://www.insideradio.com/free/bilingual-emergency-alert-gets-first-test/article_fdaf3012-8f71-11e5-8b8f-13edf6bfbc31.html;

[16] "Ohio Educational TV Stations to Strengthen Emergency Public Information System," Government Video, March 25, 2016, http://www.governmentvideo.com/article/ohio-educational-tv-stations-to-strengthen-emergency-public-information-system-/115802; "Triveni, DAS Team On Ohio Digital EAS," TV Technology, March 24, 2016, http://www.tvtechnology.com/news/0002/triveni-das-team-on-ohio-digital-eas/278247; "Triveni Digital Teams Up With Ohio Educational TV Stations and Digital Alert Systems to Strengthen Dissemination of Emergency Public Information," Broadcasting & Cable, March 23, 2016, http://www.broadcastingcable.com/thewire/triveni-digital-teams-ohio-educational-tv-stations-and-digital-alert-systems-strengthen-dissemination-emergency-public-information/154934.

[17] Deborah McAdams, "Triveni Digital and Digital Alert Systems Team Up to Add M-EAS Capability: Enables support for ATSC PSIP, ATSC Mobile ESG, and M-EAS," TV Technology, 8 December 2013. http://www.tvtechnology.com/equipment/0082/triveni-digital-and-digital-alert-systems-team-up-to-add-m-eas-capability/222701.

[18] "NAB 2016: Seven Vendors Team Up on ATSC 3.0: Digital Alert Systems, Dolby, GatesAir, Harmonic, LG, Triveni and Zenith," TV Technology, April 17, 2016, http://www.tvtechnology.com/atsc3/0031/nab-2016-seven-vendors-team-up-on-atsc-30/278491; "Broadcast Technology Innovators Team Up for Live Demonstrations of ATSC 3.0 End-to-End Workflows at the 2016 NAB Show," Broadcasting & Cable, April 19, 2016, http://www.broadcastingcable.com/thewire/broadcast-technology-innovators-team-live-demonstrations-atsc-30-end-end-workflows-2016-nab-show/155747.

The extent to which these types of industry innovations may be adversely impacted, enhanced or inhibited by changes to the nation's EAS architecture – including its constituent components – is a topic very worthy of consideration by an industry forum of EAS stakeholders.

17 Monroe Electronics support the concept of operational improvements to the EAS, however we urge the Commission to first confer and coordinate with the range of stakeholders in the design and development of conceptual enhancements or upgrades to the EAS. It is essential that such an industry forum determine the technical aspects of an enhanced EAS.

Monroe Electronics appreciates the forward-looking questions of the FCC in regards to the applicability of software defined networking (SDN) and virtualization to EAS. The proposals and questions posed by the FCC in regards to future architectures for the nation's EAS deserve broad-based consideration by the full range of EAS stakeholders. Concepts like software defined networking and virtualization may present some benefits, but will also pose very real challenges that would require interactive discussion among stakeholders to truly flesh out. The discussion of virtualization runs into a practical reality where there are functions that should not be virtualized for reasons of security, performance, individual operational requirements of EAS Participants, and other factors. There are also numerous core functions that cannot be virtualized, simply because not all functions or physical interfaces are virtualization-friendly.

The Commission's interest in such advanced architectures may reflect recent industry discussions about cloud-based and virtual services being considered or utilized by broadcast operations. However, it is important to consider that in

many cases: (1) these virtualized services are targeted to internal or enterprise clouds, which do not relate to external services, and (2) virtual or cloud-based service initiatives which are external – such as access to non-real-time programming, advertising, or front office functions – but which have no bearing or relationship to an EAS Participant's emergency communications functions.

Monroe Electronics believe it is essential for industry to have a forum to discuss and debates the relative merits of the FCC's proposals, and coordinate in depth of the technical, operational and policy implications of such far-reaching changes to the nation's EAS. We also strongly believe that many of the proposals and questions in this area will broadly impact internal systems across the nation's broadcast and cable operations. As such, it is essential that these innovations be industry-defined and industry driven.

Monroe Electronics currently provides a variety of advanced emergency content distribution and management tools integrated within the complex operational environments of numerous EAS Participants. These types of tools – which are a critical part of EAS Participant architectures – could be compromised under the alternative architectures posited by the Commission with the resultant and very substantial cost burden falling upon EAS Participants and Monroe Electronics to modify and perhaps completely replace substantial architectural elements. The economic and operational costs of fundamental changes to EAS Participant's internal operations must be considered, as well as the costs of inhibiting advanced development which is already occurring between certain EAS Participants and their respective EAS vendor-partners.

The successful development of the Wireless Emergency Alerts (WEA) system should be considered aa a reference and best practice in allowing industry to

develop the architecture and technical mechanisms for delivery of life saving alerts. Monroe Electronics urge the commission to leverage a similar approach to the question of whether and how the Emergency Alert System should be enhanced, under which industry provides the requisite technical and operational input and recommendations.

The Wireless Emergency Alerts (WEA) system was developed as the result of a broad-based deliberative process under the Commercial Mobile Service Alert Advisory Committee (CMSAAC). The results of CMSAAC also entailed incorporation of existing industry standards, and the creation of new standards as needed, where industry deemed appropriate.

The success of CMSAAC demonstrates the important role such a stakeholder forum could play in the context of the Emergency Alert System. The CMSAAC was composed of a broad group of stakeholders, which engaged in extensive discussions before submitting its recommendations for a Commercial Mobile Alert System to the Commission.[19]

The CMSAAC process was successful in large part due to the cooperative efforts of all affected stakeholders and due to the fact that recommendations generated from the CMSAAC were delivered through consensus (though not necessarily unanimous) decision making. The Commission could emulate the success of this model by establishing a working group charged with examining ways to enhance

---

[19] The CMSAAC report provided recommendations on the deliverables requested by the FCC and specified in the WARN Act, and these recommendations were generally adopted by the Commission in its First Report and Order. The Commercial Mobile Alert System, First Report and Order, 23 FCC Rcd 6144, 7 (2008)

the nation's Emergency Alert System. The Commission could charge the working group with producing reports by certain Commission-set deadlines. By so doing, the Commission would ensure that affected stakeholders have the opportunity to evaluate solutions for an enhanced EAS.

While some aspects of future architecture alternatives suggested by the FCC may provide value, Monroe Electronics is simultaneously concerned that some aspects of SDNs involve operational and system costs that may dramatically outweigh any potential benefits. We are cautious about concepts that may not function as desired – or without excessive hardship - within real-world broadcast and cable plant. These are just some of the complexities associated with adopting an enhanced EAS architecture that a stakeholder forum could most appropriately address.

It is critical that any forum or working group include all interested stakeholders, including EAS manufacturers, cable and IPTV operators, state and federal agencies, and other entities. Many of these entities had not historically been represented in the NAC, and for this reason Monroe Electronics supports re-establishment of the NAC only if it is reconstituted to adequately represent the broad base of EAS stakeholders, and possesses a sufficient degree of independence to objectively examine the question of improvements to the national EAS architecture.

Similarly, bodies such as CSRIC may not adequately represent the representative base of EAS stakeholders – and further may represent a host of entities that are not necessarily stakeholders in EAS at all. For a variety of reasons, we do not believe that CSRIC can provide the best venue for such discussions. We suggest unless the NAC is both re-established and

fundamentally reconstituted, than a separate multi-stakeholder forum beyond either the NAC or CSRIC may be necessary.

18 Conclusion

Monroe Electronics appreciate the efforts of the Commission in its desire to improve the nation's public warning capabilities. Existing EAS capabilities, including the broadcast EAS relay itself, can be significantly enhanced through relatively modest measures, as we've described above. We firmly believe that the broadcast EAS relay is an indispensable part of a robust national public warning capability, and at the same time we believe that it can be enhanced to both improve its security and the information it can convey relative to CAP.

Monroe Electronics urges the Commission to initiate a process that will enable affected stakeholders to work together to reach consensus regarding any recommendations for operational or architectural changes to the EAS that may be adopted in the future.

Respectfully Submitted,

Edward Czarnecki
Senior Director – Strategy and Global Government Affairs
Monroe Electronics, Inc.