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

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| PSHSB requests comment on impact of unauthorized EAS alerts, etc. | ) | PS Docket No. 14-200 |
| | ) | |

Monroe Electronics, Inc. respectfully submits these comments in response to the Public Notice issued by the Public Safety and Homeland Security Bureau ("Bureau") in the above-captioned proceeding, in which the Bureau seeks comment on the impact of unauthorized EAS alerts and related questions..

## I. Prefatory Comments

On October 24, 2014 at 8:21 am EDT, unauthorized EAN alert tones were transmitted in several states. The specific states and markets in which this EAN message was transmitted were unknown to Monroe Electronics at the time. The incident occurred when a syndicated radio broadcast inappropriately transmitted a recording of an EAS alert with an Emergency Action Notification (EAN) event code. Our understanding is that these EAN alert tones were monitored by certain models of EAS equipment, which then immediately broadcast the EAN emergency message.

A number of downstream EAS devices provided by Monroe Electronics monitored these EAN transmissions from upstream EAS monitoring sources. It is our understanding that no EAS device manufactured by Monroe Electronics transmitted an EAN message on October 24th or at any time thereafter.

These comments cover the following principal topic areas:

- The circumstances surrounding the events of 24 October, and the behavior of, and impact on, certain EAS units;
- Mitigations already issued by Monroe Electronics to preclude this type of event from recurring within its systems;
- Recommended improvements to the EAS to enhance authentication and, by extension, the security and reliability of the EAS;
- The government advisory to implement a so-called "strict-time" feature, if available; and
- Additional concerns regarding EAS message time and EAS device time.

## II. Initial Observations

The FCC has inquired to what extent EAS Participants had been directly affected by unauthorized EAS alerts, including unauthorized EANs, and how EAS equipment has responded.

We offer the following initial observations:

On 24 October 2014 an unauthorized broadcast of EAN tones was relayed via syndicated programming. Certain broadcast monitoring sources played those EAN tones, which were monitored by EAS devices in their facilities. Equipment settings in some EAS encoder/decoders allowed the immediate broadcast of this EAN, even though the date indicated in the alert (the JJHHMMM timestamp) was November 9th.

No EAS unit provided by Monroe Electronics or its Digital Alert Systems subsidiary broadcast the alert on 24 October 2014.

Further, it is our understanding that no EAS unit provided by Monroe Electronic or its Digital Alert Systems subsidiary broadcast a queued alert on 9 November 2014.

A number of Monroe EAS units received the erroneous EAN tones from upstream monitoring sources. We understand that a very small number of EAS devices retained the alert in queue (pending a future date of 9 November). We further understand that all these queued alerts were simply removed from the queue prior to 9 November, per instructions provided by Monroe Electronics.[1]

As noted, Monroe invested a significant effort to approach all its users nationwide on this issue, while in fact only a small number of units were impacted. At the time, we found it prudent to issue an extensive outreach effort on this issue, because it was unknown to us at the time, and for approximately two weeks afterwards, which specific markets may have been exposed to the unauthorized EAN tones. As it turned out, the number of EAS devices that retained an EAN in queue were quite minimal, and all successfully deleted that EAN before it would have been transmitted.

We deeply appreciate the efforts of the Commission, the Federal Emergency Management Agency, and a multitude of EAS stakeholders in rapidly communicating instructions on how to inspect for the possibility of a queued EAN alert, and simple elimination of that alert from the

---

[1] Monroe Electronics, Inc., Digital Alert Systems, "Cancelling Unauthorized EAN Queued Event" (2014), (http://www.digitalalertsystems.com/pdf/DAS%20FSB-103014R1.0.pdf).

queue. In particular, we note the support of the National Alliance of State Broadcast Associations, National Association of Broadcasters, Society of Broadcast Engineers, National Cable Telecommunications Association, and Society of Cable Telecommunications Engineers.

While the outreach was broad (perhaps overly so in retrospect, necessitated by a lack of initial information on the impacted markets), this outreach effort did highlight the continuing partnership across industry on EAS-related matters, and may also point to industry's own ability to manage time-sensitive communications relating to other EAS matters (including security and threat information).

## III. Monroe Electronics' Technical Response (Mitigation)

Well before this October 24th event, Monroe Electronics had undertaken actions to prepare a technical solution to preclude the recurrence of this type of scenario:

Monroe Electronics' software update version 2.6, available to all users of its DASDEC and One-Net equipment, revises handling of the EAN alert, eliminating queuing, and broadcasts an EAN alert immediately upon receipt (insofar as the alert is received within a valid time period). As the FCC has clarified, EAN alerts must be broadcast immediately (per §11.54), but all EAS headers much be utilized as well (per §11.31). As such, this update is designed to closely adhere to the Commission's rules. This software update will be available without charge to any registered user of the company's EAS solutions.

For users of this equipment that are for whatever reason unable or unwilling to update to version 2.6, we have already communicated guidance to users on how to inspect for the presence of a queued alert, and very simply delete that queued alert.[2] This guidance remains available to users as a resource. All prior software versions (version 2.5 and earlier) strictly adhere to time.

## IV. Improving Message Authentication.

The FCC asked what actions can be taken, either technically or operationally, to enhance EAS alert authentication. Monroe Electronics has suggested the addition of a message ID and/or authenticator in the EAS alert header, or ancillary to the header. Monroe has raised this suggestion in multiple fora, including the FCC's CSRIC III and CSRIC IV.

---

[2] Monroe Electronics, Inc., Digital Alert Systems, "Cancelling Unauthorized EAN Queued Event" (2014), (http://www.digitalalertsystems.com/pdf/DAS%20FSB-103014R1.0.pdf).

As discussed in detail below, the question of message authentication must relate to two systems: CAP and conventional EAS.

### *A. CAP Message Authentication*

FEMA IPAWS provides a digital signature and other means of message authentication for CAP alert messages. Many state and local CAP systems use similar authentication mechanisms, often sharing the same digital certificate as the FEMA IPAWS system. Monroe Electronics recommends that any CAP message received for purposes of EAS transmission must contain a valid digital signature for authentication, preferably an IPAWS-issued digital certificate.

One method used by Monroe's EAS to authenticate CAP messages involves inspecting the digital certificate of the received alert. Monroe's EAS equipment will reject and log any CAP message received that does not contain a valid digital certificate.

Note: Because some state and local CAP systems do not use digital signatures in their messaging, the user may elect to not filter on digital signatures for selected CAP monitoring sources. All IPAWS-originated messages, however, require digital certificate authentication.

Monroe recommends that all CAP messages intended for EAS distribution must be required to pass digital signature authentication, regardless as to whether the monitoring source is FEMA's IPAWS or from alternative state/local CAP alert services. Monroe recommends that all EAS equipment only accept a CAP message for EAS dissemination that contains a digital signature.

### *B. Conventional EAS Authentication*

We remain convinced that the conventional EAS system serves an irreplaceable purpose as part of a survivable all-hazards warning system, at both the national and local levels.

However, for conventional FSK-based EAS messages, there is no existing means of confirming authenticity. As illustrated during the 24 October event, there is no mechanism for authenticating an unauthorized EAS transmission that emanates or propagates over EAS monitoring pathways. Monroe provides suggestions below on modification of the EAS Protocol to accommodate much needed capabilities for authentication of EAS FSK messages.

Improving the security and reliability of the nation's EAS can be accomplished via modest amendment to the EAS (FSK) protocol, and in most cases may take only a software/firmware update on the part of EAS manufacturers, EAS participants, and EAS originators. We acknowledge, however, that there may be limitations on the part of some EAS stakeholders in their ability to update internal systems to accommodate such changes, such as those maintained by the National Weather Service. As such, we also acknowledge that, while necessary, such

modifications to the EAS Protocol may challenge the capabilities and resources of some EAS stakeholders in the short term.

1. We recommend that the EAS protocol should be revised to include additional authenticator either within the EAS header, or as FSK tones within the audio portion of the message, which could take the form of a unique message ID, or an authenticator. For instance, by using Textual Data Exchange (TDX), Monroe has successfully utilized FSK data in the audio portion of the message, to provide key information to be decoded downstream, without modifying the present EAS header.[3] Even several bits of data could suffice as an authenticator value that would not overly burden the EAS message and would significantly improve message security.
2. We recommend that the EAS protocol should be revised to include a "year" parameter, whether in the timestamp itself (e.g. amending it to be JJHHMMMYY), or by including a "year" as a separate header parameter, or as FSK tones within the audio portion of the message. As above, TDX could readily accommodate a "year" parameter, even if the data were merely the last two digits of the calendar year. Again, this would be a trivial amount of data to relay by FSK (and CAP) and would be of immense value in increasing the reliability and security of the EAS, particularly if additional live-code EAN tests are to be conducted in the future (and ostensibly stored with the potential of accidental or malicious replay).
3. We recommend that added authenticators in the EAS protocol be synchronized/ shared with authenticators either currently used in CAP messaging, or with additional authenticators that can be readily added to CAP messaging.

EAS Textual Data Exchange (TDX) can help carry additional data (message IDs, authenticators, year date, etc.) that would simply, effectively, and significantly enhance the ability of EAS alerts to be authenticated and properly filtered. TDX allows extra details to be encoded into conventional broadcast EAS alert messages, without modification of the EAS protocol. TDX is a text transmission technique that allows event specific details to be included in the EAS message. TDX process places a data packet within the audio envelope of the EAS protocol, and therefore does not change the existing EAS protocol, providing compatibility with legacy EAS. The TDX packet, placed before, during, or after any associated audio message, can be of short enough duration so as not to be objectionable to the listener, and will not limit the event related audio. With modern CAP EAS equipment support for the TDX approach may be a matter of software update.

---

[3] 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).

Again, while modifications to the existing EAS protocol may pose challenges to some EAS stakeholders in the short term, we feel strongly that such modifications are necessarily for to improve the security and reliability of the nation's public warning capabilities.

## V. Regarding recommendations to implement so-called "strict time"

Monroe offers the following observations about the use of so-called "strict time" filters on EAS equipment, including FEMA guidance that EAS equipment be programmed with these filters as a short-term fix.

The call for programming of "strict time" filters was well-intentioned, but unfortunately problematic, as the so-called "strict time" is a "feature" provided by only one manufacturer of EAS equipment. One the one hand, this is a key semantic issue, as the desire to ensure that devices adhere "strictly to time" could be – and was – confused with one particular product's feature that is referred to as "strict time." This had an impact discussed further below.

On this other hand, this is more than merely a semantic issue. The referenced concept of "strict-time" is unique to that particular device, and is not utilized by any of the other principal manufacturers of EAS equipment. Specifically, this particular interpretation of "strict time" relies on assumptions not shared by other manufacturers, which we understand rely on "absolute time" or "device clock time".

As a consequence, our understanding is that the government's call for EAS Participants to implement a "strict time" filter had the unintended consequence of distracting resources from many EAS Participants and EAS manufacturers who do not support this single-vendor feature. This government action imposed a measureable cost of several man-days of our technical/customer support time on the part of Monroe Electronics alone, as we fielded hundreds of inquiries from customers regarding a feature supported only by one other manufacturer. Given the number of inbound inquiries on this topic, we can but speculate on how many hundreds of cumulative man-hours were spent by EAS Participants and other EAS equipment manufacturers, responding by a Government suggestion to seek a particular configuration option only offered by one manufacturer.

Monroe Electronics has not implemented, nor does it have any plans to implement, the referenced manufacturer-specific setting of "strict time" which, in our opinion, imposes a rather arbitrary window within which an EAN is valid.

Monroe Electronics EAS equipment does strictly utilize time in the validation of EAS messages, which precluded the immediate forwarding the unauthorized EAN of October 24th. In addition, we are implementing a rigorous validation mechanism for EAN messages that we believe to be

more consistent with Part 11 rules, which ensures EAN alerts are broadcast immediately (per §11.54), within a validation window consistent with the EAS header requirements set forth in Part 11 (§11.31), and does not hold EAN alerts in queue for a future date,

## VI. Concerns regarding EAS message time and EAS device time

As noted, Monroe Electronics is issuing a device software update to revise EAS handling to allow immediate transmission of an EAN, adhering to all EAS header elements, while guarding against erroneously formatted messages, including incorrect timestamps, such as was circulated on 24 October 2014. This update allows immediate transmission of an EAN, while accommodating a controlled allowable offset, and precludes any queuing of an EAN message. This update adheres to all header elements of an EAS message.

In a previous filing, Monroe had advised the Commission of the presence of a time setting in certain devices that would allow an EAS alert to be transmitted regardless of the timestamp in the header of the message.[4] This particular setting apparently allowed the unauthorized EAN of 24 October 2014 to enter the EAS relay in several markets.

We had previously noted broadly similar situations in which an EAS message originator had transmitted messages with a "time of transmission" that was substantially in error (several months in advance of the actual date, in one instance).[5] It had been reported to us that at least one design of EAS encoder/decoder provides for an option to actually ignore the "time of transmission" – an option sometimes referred to as "fuzz" time. EAS participants using this option were apparently able to relay RMTs and other EAS events, even with an incorrect time in the header.

Our understanding is that those EAS devices that utilized "fuzz" time (or ignored time) were able to transmit and propagate the EAN alert on 24 October 2014, even though the alert contained a time stamp of 9 November. In our opinion, the existence of this option was the principal reason why the false EAN tones broadcast on 24 October 2014 were allowed to enter the EAS relay system. As noted in our previous ex parte, this utilization of this "fuzz" time feature has caused significant interoperability problems for EAS devices in the field.[6] As we commented previously, we still believe that the practice of ignoring the JJJHHMM "time of transmission" is problematic, and may in fact reduce levels of security, message effectiveness and coordination.

---

[4] Monroe Electronics, "Re: National EAS Test Findings and Recommendations, EB Docket No. 04-296," 15 December 2011. (http://apps.fcc.gov/ecfs/document/view?id=7021750843)

[5] Ibid.

[6] Ibid.

Fortunately, a dialogue has since commenced among several EAS manufacturers to attempt to create a common technical understanding and convention for time handling of EAN messages. We, and other EAS manufacturers, would endeavor to keep the Commission apprised of our findings and results.

## VI. Conclusion

We appreciate the challenge that the Commission faces in crafting policies in an increasingly complex EAS environment. We have already taken several measures to help ensure that issues such as recently encountered do not recur. We have also offered several suggestions – such as a making digital certificate validation mandatory for CAP messages, and modifying the EAS protocol to enable message authentication – that are technically feasible and in most cases can be accomplished via software update.

Though the EAS and its various components have demonstrated a number of issues over the past few years, we note that the particular EAN capability has been relatively untested in a live operational environment. While these various issues are unfortunate, and have led to some public concern, we would be mindful that many of these issues are the result of what is effectively a "shaking out" of a rather diverse and complex EAS system - albeit by means of some unconventional and unauthorized events. We remain optimistic, however, that the end result will be much greater system security, reliability and interoperability. We believe we share a common interest with the Commission, that the security and reliability of the EAS must be enhanced, while balancing against any undue burden on EAS Participants and other stakeholders.

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

/s/ James F. Heminway
Chief Operating Officer
Monroe Electronics, Inc.