BEFORE THE FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of Unauthorized EAS Alerts To: The Commission	)))))	PS Docket No. 14-200

COMMENTS OF THE BROADCAST WARNING WORKING GROUP (BWWG) RE:

PUBLIC SAFETY BUREAU REQUESTS COMMENT ON IMPACT OF UNAUTHORIZED EAS ALERTS ANDANNOUNCES INQUIRY INTO CIRCUMSTANCES OF RETRANSMISSION OF UNAUTHORIZED EAS MESSAGE IN SEVERAL STATES

I. Preface

The Broadcast Warning Working Group (BWWG) core membership consists of hands-on Emergency Alert System (EAS) subject experts from the fields of broadcast association management, broadcast radio and television engineering management and support, radio and television news, industry technical publication, and state EAS Committee leadership. The BWWG hosts a website, the EAS Forum at:

[http://eas.radiolists.net/]

II. The Public Safety Bureau has asked for Comments that answer the following questions:

A. To what extent have EAS Participants been directly affected by unauthorized EAS alerts, including unauthorized EANs and To what extent have National Primary and Local Primary EAS Participants been affected by unauthorized alerts?

National Primary and Local Primary EAS Participants are vital to the current EAS infrastructure. Without their voluntary cooperation, the current EAS structure is at risk. While the stations that participate in the Primary Entry Point program (PEP) have signed contracts and have accepted significant upgrades to their on-air infrastructure, there is nothing to prevent any or all of them from opting out if EAS carriage is seen by them as a detriment to their on-air operations or an excessive expenditure of their own resources. Contracts can be abrogated.

While non-PEP licensees should consider the unfunded mandate that is the EAS as part of their responsibilities to their audiences, the real dollar costs to licensees when things go wrong certainly diminishes their commitment to this form of public service. Since the Commission has not yet seen fit to standardize the way EAS Participant devices behave, and there was predictable early confusion on the extent to which the bogus event had propagated or might propagate, much time and effort (read dollars) had to be devoted to responding on short notice. This is especially important to keep in mind regarding the EAN code that is "must carry" and, by design, is not subject to any significant degree of oversight by EAS Participants before airing.

B. To the extent EAS Participants have received unauthorized EAS alerts how has EAS equipment responded?

The BWWG knows from postings on the EAS FORUM that EAS different equipment responded in different ways to unauthorized EAS alerts. We feel the FCC should seriously consider standardizing how EAS equipment responds to all EAS events in the future. We know this will not be an easy, painless nor inexpensive process. Further, no changes the Commission decides to implement will have any binding effect unless an overall EAS certification process for all vendor equipment EAS behaviors is put in place. Having certification only for Common Alerting Protocol behaviors is simply not enough – especially as long as Legacy EAS is still with us. Yes, the Commission should allow manufacturers to implement their own feature sets. We suggest a requirement that a 'radio' feature set should not impact a feature set for 'cable' or 'TV', and conversely.

C. How does EAS equipment handle the absence of an End of Message (EOM) code?

There is a two-minute "time out" built in to all EAS devices that will automatically terminate all but EAN alerts. A missing EOM on an EAN will leave downstream EAS Participants connected to the EAN source they are monitoring.

D. How do EAS Participants determine the authenticity, or lack thereof, of an alert message?

There is currently no way to do this, nor is there an easy way short of expensive changes to or replacement of the receiving equipment. The receivers are programmed to receive certain events and how to handle them when they are received. If a "fake" EAS event is sent or an operator make a mistake but has the right credentials and timestamp, it will be propagate as programmed, even if it is a recording of a previous alert. Of course, the timestamp is irrelevant for EAN, as the Commission requires "immediate" forwarding.

E. How is EAS equipment programmed to manage message authentication?

Since the stations are programmed according to the State Plan, stations rely on their LPs to control/vet/ and ensure only authentic messages are sent. (CAP EAS messages propagate directly to all broadcasters, according to the way stations have set their filters.) If a fake event comes from an LP, there is nothing standing in the way of the event propagating to all EAS Participants who monitor it. Additionally, the use of YouTube audio on a satellite-fed program bypasses this issue.

F. There have been several stories in the press and on listserv discussions about the use of "strict time" filters on EAS equipment. Indeed, FEMA staff recently recommended that EAS equipment be programmed with these filters as a short-term fix.

For the EAS EAN event code, strict time is a moot issue. All EAS Participants must relay EAN's when received. The discussion about strict time is, as far as the BWWG is concerned, thoroughly settled. Strict time is more than adequately defined in Part 11 and must be considered an absolute, hard EAS requirement. Interpretation of strict time in filters should never be permitted[1] since EAS installations configured to poll one or more CAP servers are by definition connected to the Internet and can and should be set to receive any number of accurate time servers. If so connected, even if a Wide Area Network (WAN) connection is lost, the internal clocks for EAS devices will keep time closely enough for proper EAS propagation.

For all other alerts, every LP station is now connected to the Internet and accurate time is nearly universal. If an EAS Coded alert arrives with a non-current time stamp, it should be rejected.[2]

G. To what extent, if any, have EAS Participants implemented this recommendation?

Without a survey to make sure that EAS devices that can deviate from strict time do not, we cannot say.

H. More generally, what actions can be taken, either technically or operationally, to enhance EAS alert authentication?

The next logical step is to use a class of devices we can call warning appliances that can get information-rich CAP-based messages to the public without interrupting ANY on-air program stream unless truly necessary. Such devices will poll CAP servers as well as legacy EAS sources and display as much or as little information on displays ranging from tiny LCD screens, scrolling video messages, on to devices that can work with home video and audio entertainment systems.

---

[1] The only exception might be for EAS Participants that have received waivers from the Commission due to their inability to obtain WAN connectivity.
[2] There may be occasions where the clocks at an isolated station or emergency management agency are out of sync, but this would normally be uncovered during regular weekly/monthly testing.

The "Virtual Red Envelope" (VRE) that has been proposed is an automated message validation concept that gets its name from the Cold War-era EBS red envelope which contained codes to validate national activations. This system was never used for a real EBS event.

The proposed VRE system would use the IPAWS servers to distribute a short validation code as part of the Required Weekly Test. Upon receipt of an enhanced single location EAN, EAT, and NPT message created only by the Presidential Entry Point system and authorized test encoders, recipient equipment would compare the validation code of the enhanced message header to the prior downloaded and locally stored code. A code match would compel the recipient equipment to automatically and immediately proceed to forward the entire enhanced EAS message in accordance with Part 11 requirements. A non-match would trigger an alarm requiring manual review of the message for verification of origination. To maintain complete conformance with the SAME coding standard, the validation field would be appended at the end of the EAS message header.

The single location code EAN, EAT, and NPT message types would trigger the recipient equipment to accept the added field for decoding and validation. To minimize erroneous matches, missed code circulations, and the staggered weekly test schedule based on time zone, the system would include the three most recent weeks validation codes. The EAS message's enhanced header would include all three week's codes in the field. If any of the three codes match, validation would occur. Additionally, recipient equipment that determines that the validation code has lapsed could poll IPAWS for that week's validation code.

I. What control mechanisms do EAS Participants and their industry associations have in place to assess network integrity, accepted risk, and effectiveness of mitigation measures?

The BWWG, among others, hosts and maintains an information exchange forum for EAS participants, public/private stakeholders, and vendors. State broadcaster and cable associations help to distribute information to EAS Participants. CSRIC has and will continue to offer guidance.

A good start would be to have regular reports from each state, indicating the penetration of each RMT. Stations that do not receive the RMT regularly should be assisted to promptly resolve the issue.

That said, when the Commission is slow to respond and does not coordinate their response with their Federal partners, distribution of late and uncoordinated information to the EAS community could only add to uncertainty and confusion. The BWWG sees a need to resurrect the model that brought CAP into being, the Partnership for Public Warning (PPW). An independent PPW can look at the overall integrity of the public warning effort in ways that CSRIC, the BWWG, and state broadcaster associations cannot.

J. What impact does public safety agencies and other state and local government agencies experience when there is an unauthorized EAS alert?

Public safety and local government suffer collateral damage whenever EAS glitches happen. The most visible sign of this damage is a burden on 9-1-1 and other public contact means. Less visible harm but nonetheless significant is overall erosion of confidence in the use and support of the EAS. This cannot be allowed lest EAS lost the support of the very people at the local level who should be using it at every opportunity as a core emergency response resource.

K. Is the impact different if it is an EAN alert?

If a successful EAS event propagation leads to getting protective actions to a public at risk, this builds confidence in the value of the EAS as a viable response tool to help save lives and property.

L. What actions, if any, have state and local governments, including public safety agencies, taken to mitigate public confusion when there have been unauthorized alerts?

As far as we know, no comprehensive survey has been done yet. Revival of an entity like the Partnership for Public Warning (PPW) can help.

M. Were any of these actions part of a joint effort with EAS Participants and/or Federal government agencies? If so, were those efforts effective? What actions do such agencies plan to take in the event of an unauthorized alert in the future?

The Commission needs to promptly identify what is expected of state and local EAS committees and what they want the State Plans to communicate to each state's EAS Participants.

N. What additional actions, if any, can be taken in the future to avoid or mitigate the effects of an unauthorized alert?

Education of licensees and their air staff is essential.

Fast issuance of Public Notices and much-needed coordination between Federal partners will help the overall effort. The opposite will make things worse.

O. What actions should government agencies and EAS Participants take to better educate the public about the EAS?

In the case of the fake EAN, the education needs to be at the station and corporate level. The Commission might investigate whether it is appropriate, either for the FCC or stations involved, to require *YouTube* and other similar sources of video and audio clips to pull down the clips with EAN tones in them – or at least muddle the audio.

P. What effect, if any, do unauthorized alerts have on members of the public, including those with disabilities and those who do not speak English as a primary language?

The confusion is palpable. However, this is not limited to the recent fake EAN. Nearly every month at least one area reports EAS tests that have gone wrong and an erroneous EAS alert issued by mistake. Steps need to be taken as soon as possible to reduce these mistakes and errors. The operation of stations has changed dramatically since 1994, and Part 11 should recognize that now – not in a few more years.

III. Conclusion

A. The Commission has in this item asked EAS Stakeholders to answer a number of questions. The BWWG believes that while the answers to these questions that the BWWG and others provide is useful information, it only deals with one challenge to improving the EAS. The BWWG strongly recommends that the Commission look beyond this single issue if the EAS is to survive as a viable public warning resource.