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

In the Matters of	)	
	)	
Amendment of Part 11 of the Commission's Rules	)	PS Docket No. 15-94
Regarding the Emergency Alert System	)	
	)	
Wireless Emergency Alerts	)	PS Docket No. 15-91

Comments of Sage Alerting Systems, Inc.

June 8, 2016

Contents

1 Introduction 1
2 Improving EAS Network Security 2
3 Securing EAS 3
3.1 Background 3
3.2 Replay Alerts 4
3.3 Issuance of an alert by an authorized person that is incorrect 5
3.4 Issuance of an intention unauthorized alert for relay 5
3.5 Recommendations for securing EAS 7
4 Maintaining legacy EAS in an IP world. 8
5 Centralized configuration and management 9
6 Comments to specific questions 10
7 Comments on proposed rule changes 14
8 Conclusion 17

1 Introduction

Sage Alerting Systems has been active in EAS and emergency notification and warning since the pre-EAS field trials in the early 1990s. Sage has worked closely with the FCC, FEMA and local emergency management agencies to improve the delivery of warnings to the public, including work on the FCC's CRSIRC advisory committee and the EAS-CAP industry group.

Sage welcomes the Commission's efforts to improve the EAS system and makes the following comments and recommendations on some of the wide-ranging issues the Commission has brought forth in its Notice of Proposed Rulemaking.

2 Improving EAS Network Security

Sage will not presume to estimate the costs for EAS participants to assess whether or not they are following best practices, and if they aren't, to implement those practices. We do know that some users continue to struggle with basic network connectivity and security. We hope that most of these participants are at the far ends of the chain with no one using them as a monitor source so the impact of any breach will be small, but there is no guarantee that this is always true.

Asking stations to certify that they are doing the right thing, under penalty of perjury, is one approach. For best results, this must be combined with help. The FCC and industry organizations must continue the outreach and develop tools and resources to help them do the right thing.

For example, in para 123, the FCC proposes that a participant certify that their EAS device is not directly accessible through the Internet, for example, by configuring a firewall to deny access from the public Internet. This presents a significant barrier to participants that must depend on an outside consultant to apply patches, retrieve logs, change filters, update source PSID lists, etc. The ongoing costs for a VPN or a white list could be significant.

Sage plans to provide an assessment tool for its users that will check the Sage ENDEC's configuration, check for patch level, password refresh, digital signature validation settings, and any other FCC mandated certification topics, so that minimally trained users can easily gather the information they need about the state of their Sage ENDEC. It won't help configure a VPN, but it will reduce the recurring cost of yearly certifications, if that is the path the FCC pursues.

Sage recently worked on the CSRIC V WG3 EAS Handbook committee to develop an updated EAS Handbook. One goal was to assist "less resourced" EAS participants in understanding what the basic functions of EAS are, and how to develop procedures

necessary to meet the FCC requirements. Sage recommends that a similar task be undertaken to help the less resourced meet their security obligations.

3 Securing EAS

3.1 Background

The primary focus of Sage's comments herein are for the legacy EAS, by which we mean the over the air relay of alerts from one EAS participant to another over an unsecured public audio link. CAP message authentication, as defined in the CAP protocol, is fully supported by the Sage Digital ENDEC.

All EAS participants must be able to receive and process CAP-based EAS alerts, and a majority of them do. Some EAS participants have waivers, but the majority of EAS participants are now able to directly access the richer information in the CAP version of the alert. One role of the legacy EAS system is now as a backup when the Internet is not accessible.

As a backup to the Internet, it doesn't make much sense to add data to legacy alerts that would allow them to be authenticated by checking the Internet.[1]

Not all EAS alerts are accessible on a CAP server. Some are issued only as a native EAS alert. These include:

- Alerts originated by a county that does not have the ability to issue a CAP message, but does have the ability to issue a legacy EAS alert
- Monthly tests originated by a SR or LP station
- Alerts originated by a broadcaster at the request of an authorized local agency that does not have the ability to issue CAP or legacy alerts on its own
- Alerts issued by counties with CAP capability, but where CAP insertion is temporarily unavailable.

The major source of native EAS alerts is the National Weather Service. NWS alerts are not currently issued through the IPAWS system for EAS distribution. They are only

[1] This is not the same as checking the Internet to see if a "better" version of a legacy message is available via CAP, for those cases where the legacy message arrives first.

available as legacy EAS messages via the national system of NOAA weather transmitters.

It is not clear when weather alerts will be available on CAP for use by EAS participants. There are many complications; technical, procedural, and fiscal. But until NOAA can issue all of its alerts through CAP, or can add whatever authentication mitigations the EAS system devises to its legacy alert SAME protocol, the EAS system must still accommodate the transfer and relay of unauthenticated weather messages.

As long as the above types of "native EAS" originators exist, it will be difficult to secure the types of alerts that can be issued by such originators. It would be possible to add authentication to only the national NPT and EAN alerts.

One class of erroneous alerts that can be solved without authentication is the replay class. Another class can't be helped by authentication: issuance of an alert by an authorized person that is incorrect – issued with the wrong event type, an incorrect location, or an in-house test alert that was accidentally broadcast.

Only one class of erroneous alert must be solved by authentication: the issuance of an alert by a person who intends to issue an unauthorized alert and intends it to be relayed.

3.2 Replay Alerts

Whether a broadcaster plays a recording of an EAS alert, such as the Bobby Bones Show incident, or a news program includes an alert in its report, or an alert is contained in advertising; all appear to be valid alerts that have expired.[2] All of the problems caused by a replay can be eliminated by correctly detecting expired alerts based on the JJJMMHH field and the duration (TTTT). In the case of a relay occurring on the same date in a different year, a year code could be added to the end of the ZCZC protocol string.

Correct detection of an expired alert, as most replayed alerts would be, will remove any possibility of relaying an old alert. Sage recommends that specific details on how to compute the time during which an alert is valid, including allowance for clock slippage, become a part of the Part 11 rules, or that a technical guide, such as the 2010 EAS-CAP

[2] A replay of a valid, unexpired alert that had already been processed would be treated as a duplicate.

Industry Group's Implementation Guide, or a similar guide maintained by CSRIC, be developed.[3]

We also note that, by itself, a digital signature would not be sufficient to thwart a new Bobby Bones incident. Had the gag replayed an alert with a digital signature, the signature could still be valid.[4] Strict adherence to the valid time of an EAS message is critical to avoiding replay errors, even if the alert does contain a digital signature.

3.3 Issuance of an alert by an authorized person that is incorrect

There is little than can be done at the EAS level to detect or prevent problems caused by a bad alert issued by an authorized entity. The example cited in the *Notice* at ¶101 was **not** a case where authentication would have helped. The EAN alert was issued by an authorized person with authorized equipment, but due to a misconfiguration, it went on the air rather than to an internal test circuit. There are many examples of a "real" alert that was not intended for distribution making it on the air. There are many other examples where an authorized person issued the wrong event code, or an incorrect area, or a bad audio attachment that caused an incorrect alert to get on the air. These alerts are just as likely to be issued on CAP as they are on native EAS. Training and continued refinement of origination systems is required.

It is possible to reduce the effects of accidental alerts by restricting conditions under which the EAN, NPT, and the 000000 code are accepted. While this won't protect against intentional spoofing, it might protect against an errant key stroke. Sage recommends that the rules be changed to specify that EAN and NPT are only valid with an ORG code of PEP, and that the 000000 code can only be used with the EAN or NPT codes. Other uses of 000000, or EAN and NPT without the PEP originator code, must not be relayed.

3.4 Issuance of an intention unauthorized alert for relay

In this instance, we assume that the person involved has access to everything they need to receive legacy alerts, and to format a legacy alert of their own, either through an

[3] CSRIC IV WG3 addressed a portion of the issue, see https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-3_Final-Report_061814.pdf

[4] Depending on the signature scheme used, the signature could be valid for months or years.

FCC certified device, or software/hardware of their own devising. In this case, just as with any other digital message sent via any other unsecured transmission medium, the message itself needs its own authentication scheme, such as a digital signature, using real cryptographic techniques, to prevent an unauthorized message from being accepted for relay.

Several alternate schemes have been proposed though the years, most of which have one flaw or another. These can be summarized as:

Use of a code word that is periodically sent in advance of need and transmitted in the clear. It is also transmitted in the clear when used, and remains valid until replaced. Such a system provides little security.

Use of a very small cryptographic key. A few bits of authentication is no longer viewed as adequate in any circumstance requiring authentication.

Use of the Internet to verify the alert. As one of the major reasons for the continued use of legacy EAS is to serve as a backup to the Internet during loss of local EAS participant access, alert originator access, the CAP server, or the Internet itself, use of the Internet to verify the backup is not possible. On a good day when the Internet is up, a legacy alert can be checked – but in that case, the alert would have been accessible via CAP in the first place. An alert natively issued to EAS could not be on a CAP server. While the Internet (if available) could be used to check to see if an alert has been judged to be false, an alert is unlikely to be repudiated before most EAS participants encounter the alert and start the relay. On a bad day, the Internet may not be available.

Manual verification. Many EAS participants run unattended operations for some or all of each day; there is no operator on duty to perform a manual review. Even if an operator is present, there are few alternative authentication tools available, and the operator would have little training and less practice with manual authentication skills.

Audio-source authentication. The EAS system relies on multiple paths to provide redundancy. Each EAS participant will have at least two, and sometimes six or more, audio inputs. While it would be possible to assign an expected LLLLLLLL field to each of the sources, doing so will add fragility to the system. Those assignments will change

over time, requiring updates. Some state networks will have multiple sources on a single audio channel. Some co-owned/co-located facilities will have multiple audio outputs and multiple stations with the same LLLLLLLL field. There would be an increase in EAS system maintenance with a continuing risk that stations will be out of date on audio assignments or identifiers, resulting in the rejection of a valid alert. Using audio source authentication won't stop an intentional spoofing of a legitimate source. Its main utility would be in stopping replay errors, but those are better handled by correctly identifying expired alerts.

3.5 Recommendations for securing EAS

To ensure the greatest possible security for the legacy EAS system, we must:

1) Reduce the number of native EAS originators.
2) Use a true digital signature system to sign the alerts. Don't try to use a URL tucked away in the header that would require the Internet to be up both at the originator and the receiver.
3) Tread carefully when specifying changes that will increase the EAS participant workload, require software updates, as well as cause interoperability problems during lengthy deployment cycles. Make sure that we are actually gaining protection from intentional bad alerts, and not simply applying expensive mitigation against replay alerts where a simpler solution is possible.

Sage recommends that the legacy system be maintained as part of its original function of the EAN, now as a backup to CAP. High impact alerts such as EAN and NPT should be protected using digital signatures. Sage has used such a system with success in the past, by transmitting a group of signature frames that precede the normal set of three standard EAS headers they are protecting. This allows for unmodified devices to receive the alert at the end of a chain, while updated devices that relay the signature frames can act as relays. This provides protection for the type of alerts that can cause the most disruption. Ultimately, we should work to transition most alerts to CAP only, leaving legacy relay of alerts for EAN, NPT, and legacy transmission of RWT (for path checks).

4 Maintaining legacy EAS in an IP world.

Sage believes there is still a place for legacy EAS in a world with IP based CAP messages. Primarily it is as a backup to CAP-based EAN distribution, for use on a very bad day.

For day to day use, CAP messages would be preferred. The FCC, or a technical committee, should recommend a best practice for searching for a CAP alert that matches a legacy EAS alert when the legacy alert arrives first. This is not an uncommon occurrence, based on 30 second polling cycles, a delay of a second or two to get an alert on the air, and seven seconds to receive legacy headers, if the upstream station polls first, the legacy alert can easily be the first to arrive.

The current FCC rules specify “immediately” for some alerts. That may need to change if a delay is to be inserted to seek a CAP alert, or wait for one to arrive on a satellite or other distribution link.

Care should be taken to not allow a lengthy delay to acquire a CAP message. Not every EAS participant uses a high speed Internet connection. Some audio file servers don’t have the bandwidth to support hundreds (or thousands) of simultaneous fetches at full speed. Some satellite links deliver data at a small multiple of the encoding rate of the audio, it may take 30 seconds for a file containing two minutes of audio to download. For a variety of reasons, fetching a CAP message and its associated audio can take more than a few seconds. A time-critical legacy EAS warning delivered right away may be better than a pristine message delayed by a minute.

Sage recommends that the rules be modified to allow a search for a matching CAP message, with reasonable maximum delays.

Sage does not recommend that legacy EAS be enhanced to provide the features available in CAP, in particular, polygons, and extended text. This should remain in the CAP domain. Legacy EAS serves as a last ditch effort to provide information when other transport mechanisms have failed, and as such, should fall on the side of high reliability and less so on extensions. Additions to the EAS protocol should be carefully considered.

5 Centralized configuration and management

Would centralization improve EAS?

If the goal of EAS is to provide a backup path for EAN and other messages when a central system is down, each EAS device must be able to function independently. It can't be just a remotely controlled relay to select audio feeds.

Would it reduce user costs? Presumably, the local station is still responsible for getting alerts to air, checking logs, and updating settings to reflect changing needs. Whether this is done with a web browser pointing to the local device, or a web browser pointing at the cloud, the work load is the same.

Would it increase reliability? While the EAS device tends to get a lot of attention, the rest of the plant also plays a critical role. The EAS device interacts with switching audio, inserting video, interfacing with a variety of peripherals connected via IP, serial ports, USB, multi-station interfaces and GPI/GPO. Interface to automation systems, character generators, led signs, HD radio exporters, flashers, SMS text messages, "play it now" buttons on the web interface – all of these are locally defined, refined, and integrated into other systems. While a central system of pushing patches might improve security, much of the reliability of the EAS system is not just in the EAS device.

Can current hardware be used? Current hardware, such as that used in all-in-one CAP/EAS devices, probably. Modern devices already have the capability of handing digital signatures, audio in various formats, HTTP/SSL access, and can likely handle additional remote control features.

Does every EAS device need an Ethernet port? Yes. Also, CAP converters should be phased out.

All that said, if a large part of EAS is to provide local control, both in selecting which alerts to air, and overriding or delaying them on a case by case basis, and integrating into the local plant, centralizing the system will do little toward reducing the work load. The same people will be doing the same things, just a little differently.

From a cost savings standpoint, we need to consider what EAS tasks the local EAS participant performs, and see if moving to centralized control helps or hurts. We need to see if participants want to cede control of a cut-over switch to a black box administered remotely.

It is premature to discuss costs until we quantify the potential benefits and answer the workload questions. Assuming the central control isn't free, we are to some extent talking about augmenting existing hardware with a subscription based application. This might not lower costs in the long run.

Sage heartily recommends the discussion of the concept with all EAS stakeholders, both to determine the overall need, the effect on participant operations, and the myriad technical aspects involved.

6 Comments to specific questions

Para 32 - Should FCC reestablish the National Advisory Council (NAC)?

Yes. Membership should include EAS manufacturers, as they also have day to day contact with EAS participants at all levels, as well of a deep understanding of technical limitations and interoperability issues.

Para 66 – Use of EAS Header tones in PSAs

Sage does not see the need to use the EAS header tones in PSAs. As the attention signal always accompanies a critical alert and tests such as RMT and NPT, that is the tone the audience needs to learn. The header codes are always interpreted by hardware and software, but never by the audience, and need not be a part of audience training. There is no need to craft a special header event code or in some way damage the header so that it sounds like an alert but is not detectable. The EAS header tones should be broadcast only when they are meant to be decoded. The two tone signal should only be used for actual alerts, and sparingly for PSAs. The tones should never become commonplace, or contribute to audience tune-out.

By allowing header codes, even sound-alike tones, in PSAs and infomercials that could possibly show up unannounced in syndicated or network programs, a burden is

added to personnel at EAS participants who are tasked with keeping an ear out for a repeat of the Bobby Bones incident.

Use of header codes can cause unintended side effects, even if only to add an unusual log file entry. If headers are to be allowed, creation of a technically harmless header depends on the abilities of the person generating the audio. If the header "sounds real" to the ear, then stations previewing the PSA or sponsored infomercial would need to use an EAS device to verify that the header is harmless. The station is ultimately responsible – not the producer of the infomercial. If header codes are to be allowed, then the FCC must provide one, and Part 11 must require that only the official audio file be used for content of this type. The official FCC-provided alert must be modified in bit timing, frequency, and content, and be verified in a test facility to determine that it does no harm.

Para 110 - whether additional measures should be taken to secure particular alerts, such as the EAN

If a digital signature is used to provide authentication for an EAS alert, then the originator needs a signing key. Key management among potentially hundreds or thousands of native EAS originators could be burdensome. A less expensive solution would be to use digital signatures only for the alerts that will cause the most disruption, EAN and NPT. As these alerts would only be issued by FEMA, only a small number of locations would need the signing key.

If the EAS signature is added to a CAP message, then participants could add that signature when they transmit an EAS message derived from a CAP message. Downstream users that can't receive the CAP message could still validate the signature. This would provide protection for any EAN/NPT, as well as any alert that started as a CAP message, leaving only less disruptive messages that were originated on EAS to have no authentication.

The process of receiving a message and checking a digital signature is already required by CAP. If a similar technique was used for the EAS message, then the

additional system cost would be for a software update, no new hardware is likely to be required, provided the user is using modern CAP/EAS hardware.

Para 132 - 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

Sometimes, the root cause of the problem is upstream, and a station that "contributed" simply by carrying a syndicated show, would be unaware that a lockup problem had been caused downstream. Other times, the problem is downstream of any EAS device. Requiring that participant to meet a 15 minute deadline is unreasonable, especially if the problem occurred hours or days before.

The resources would be better spent in developing procedures to detect a lockout, and to be able to clear it without lengthy delays.

Para 136 - … we seek comment on the desirability and feasibility of discarding CAP formatted EAS alerts where the digital signature is invalid.

The Sage ENDEC already has the ability to both require a signature, and reject a CAP message if the signature is not valid. This is our recommended setting for IPAWS messages. We also have a setting to allow the ENDEC to accept CAP messages without signatures on a given server, as some non-IPAWS servers do not provide digital signatures. The user can also elect to accept messages with bad signatures. This is not recommended.

We do recommend that messages with bad signatures be discarded, this is our default. Not only does this protect against spoofing, it also verifies that the message has arrived at the ENDEC without corruption, intentional or otherwise.

Requiring all non-IPAWS messages to be signed might place a burden on origination systems that don't use signatures, but Sage certainly agrees that signed messages be a goal for all CAP message originators.

Para 137 – digital signatures for EAS protocol

Sage agrees, certainly for disruptive messages like EAN/NPT that digital signatures should be used for EAS messages as well. Our detailed comments above in "Securing EAS" provide more background. As regards the class of solutions discussed in Para 137, Sage is opposed to the use of any proprietary protocol as part of EAS. Insufficient data is present in the *Notice* to evaluate this particular example. To be considered for part of the EAS specification, Sage strongly believes that any protocol must be published openly and available to anyone. Keeping the protocol specification under limited distribution, while regularly using it on public channels, will not add to the security of EAS.

Insufficient information is available to assess the statement that "only a few bits of data could serve as an authenticator value", as "a few" is not generally regarded as cryptographically significant. We note the reports of testing with a relay through a single intermediary station, but would like to hear more about passing AFSK through several record/playback hops in a relay chain (possibly as many as three for an EAN), where the effects of receiver noise, processing, record/playback levels, and AGC are cumulative. We prefer the method used by EAS itself, where AFSK is regenerated at each hop.

That said, Sage is always willing to help evaluate and test any proposal from the FCC to help in the task of producing a more secure EAS. It is premature at this time to take a guess at implementation time and costs.

Para 138 - Virtual Red Envelope (VRE) system

This system sends code words in the clear, and can therefore easily be spoofed. The VRE concept, once deployed to all participants, would stop a repeat of the old Bobby Bones incident, but would not stop future incidents of a relay of the new format alert. The replayed alert would have an authentication code word. If the relay occurred in the same week (or month, both RWT and RMT are used in the example), the alert would still appear to be valid. Detection of an expired alert, which does not require authentication, would be the only mechanism to keep the alert off the air.

Any EAS participant that missed a code word transmission would not relay protected alerts until the code word was updated. At many stations, holding an alert for manual review isn't possible. Our detailed comments above, "Securing EAS", provide more background.

Para 143 – time stamp

Sage agrees that EAS devices should validate alerts based on the time stamp. For maximum interoperability, the FCC (or other technical group) should define an algorithm to determine time validity, allowing for legacy device clock skew. For completeness, a year value should be added at the end of the EAS protocol where it will not interfere with existing devices, but ***not*** at the location discussed in the proposed change to 11.31, as that location would invalidate all unpatched devices as well as consumer NWS receivers.

Para 144 - interstitial alerts

Sage recommends that the FCC consider using the technique described in Annex B of the CSRIC IV final report.[5]

7 Comments on proposed rule changes

11.31(c) and 11.32(5)

Sage strongly disagrees with the location of the YYYY parameter, as it is not backward compatible with unpatched devices, or with the NWS SAME protocol embodied in many consumer radios. The year could be added to the end of the frame, however, or combined with an authentication scheme. We recommend that the FCC defer this change for additional technical review. To the extent that this is meant to mitigate replay issues, a strict definition of when an alert is valid will work for most days of the year, and can be implemented without a protocol change.

[5] See CSRIC IV, WORKING GROUP THREE, EMERGENCY ALERT SYSTEM, NATIONAL TESTING AND OPERATIONAL ISSUES TASK GROUP, FINAL REPORT ANNEX B (June 2014), available at https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-3_Final-Report_061814.pdf

11.33

Rejection of a message based on monitoring sources and a white list of allowed LLLLLLLL values is costly for stations to manage and makes the overall system more fragile, as station settings, the state plan, and reality must all match. The benefits are a small incremental protection against replay errors, with no protection against intentional spoofing. Sage does not believe the cost/benefit analysis weighs in favor of this change and recommends that the concept be removed.

The phrase "expiration time is in the future" is not sufficient. Expiration time is not defined. It is JJJHHMM + TTTT (+year). The JJJHHMM + year must be in the past (plus or minus a clock skip allowance) and the expiration time must be in the future. If YYYY is not added at this time, additional explanation is required. If it is July and the alert expiration is in October, the alert should be rejected. If YYYY is added, the JJJHHMM + YYYY is far in the future, the alert should also be rejected We recommend additional technical review.

11.44 Security of EAS Participants

Some stations will be relying on an external consultant to assess compliance. Is perjury the proper penalty here?

11.46

Sage recommends that only the Attention Signal be permitted. See our discussion above on Use of EAS Header tones in PSAs. If a header is to be allowed, then the FCC should provide header audio to be used, where the audio has been proven to be harmless and undetectable by EAS equipment.

11.54 (a)

The commission may want to take this opportunity to provide additional guidance on what is meant by "NPT Event code in the case of a nationwide test of the EAS" in the context of regional tests. In plain language, an NPT sent only to Florida is not a nationwide test. Is a nationwide test only an NPT with a location code of 000000? Is a regional test treated any differently? If the intent is to treat all NPTs the same (and

Sage agrees with this), then we recommend dropping "in the case of a nationwide test of the EAS".

11.54(a)(1)

Given the automated aspect of EAS, and that the FCC in its 5th R&O states at para 61 "The Commission amends the Part 11 EAS rules so that EANs will be processed on a message-by-message basis, like any other EAS message, only on a mandatory and priority basis." What is the mechanism by which stations transmit their call letters? This section may be a carry-over from EBS and should be removed.

11.56(c) .. *EAS Participants shall configure their systems to treat as invalid all CAP-formatted EAS messages that include a digital signature that does not match an authorized source from FEMA or from a designated source as specified in the state EAS plan*

Is this meant to refer to the source of the CAP message, or the source of the digital signature certificate? Is the intent to require that the root certificate of the signing key be one of a known list? As written, the rule allows CAP messages that aren't signed, but disallows some messages that ARE signed, but are signed with a key that didn't come from a designated source. Additional technical detail is required to describe what is meant by the authorized source of the digital signature, how to identify one, and how to add it to the state plan.

An alternative suggestion:

EAS Participants shall configure their systems to accept only digitally signed CAP messages. EAS Participants shall also configure their systems to accept only digital signatures whose root or intermediate certificate is specified by FEMA, or other certificates as specified by the State EAS plan. All other CAP messages are to be discarded as invalid. If a state plan includes a CAP source that does not digitally sign messages, that source may continue to be used until one year after publication of these rules.

This may ultimately be difficult to maintain as certificates are updated over time. An additional technical review is recommended.

8 Conclusion

With this NPRM, the Commission has raised significant issues regarding the future of the EAS system. While there are some incremental steps that can be taken in the short term, many of the proposals made can offer benefits as well as disruption to EAS participants and their partners. To pick the proper path will require discussions with all stakeholders. These need not necessarily be lengthy, but early discussions on whether or not we are addressing the right problems in the right order will help us all get to the end sooner.

Sage makes no particular recommendations as to the proper venue for these discussions. As CSRIC V is up and running, it may be an appropriate first choice to at least start the discussion.

Respectfully Submitted,

/s/

Harold Price
President,
Sage Alerting Systems, Inc.