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

In the Matter of	)	
	)	
Request for Comment on the Impact of Unauthorized EAS Alerts	)	PS Docket No. 14-200
	)	

COMMENTS OF THE NATIONAL ASSOCIATION OF BROADCASTERS

The National Association of Broadcasters (NAB)[1] submits these comments in response to the Public Notice requesting comment on the impact of unauthorized Emergency Alert System (EAS) alerts.[2] The Public Notice references the improper transmission of a recorded EAS message on October 24, 2014, and seeks comment on how EAS message authentication can be improved to prevent similar situations in the future.[3] Given the complexities of these authentication issues, NAB urges the Commission to support a joint industry effort to address them.

The October 24th incident noted above involved the airing of an EAS alert recording coded with an Emergency Action Notification (EAN) code, which is the highest level EAS code and intended only for EAS alerts issued by the President.[4] The

---

[1] NAB is a nonprofit trade association that advocates on behalf of local radio and television stations and also broadcast networks before Congress, the Federal Communications Commission and other federal agencies, and the courts.
[2] PSHSB Issues Advisory to EAS Participants to Check Equipment for Possible Queuing of Unauthorized EAS Message for Future Transmissions; Requests Comment on Impact of Unauthorized EAS Alerts and Announces Inquiry into Circumstances of Retransmission of Unauthorized EAS Message in Several States, *Public Notice*, PS Docket No. 14-200, DA 14-1626 (*rel*. Nov. 7, 2014) (Public Notice).
[3] Public Notice at 1.
[4] 47 C.F.R. § 11.2(a).

Commission's rules state that EANs override all other EAS messages, and require that EAS Participants interrupt regular programming to air such messages immediately upon receipt.[5]

Broadcasters who retransmitted the October 24th message followed this required process, complying with both Commission rules and its recent declaration that "EAS equipment must transmit the EAN immediately upon receipt, regardless of the Time of Release provided by the alert originator."[6] Accordingly, NAB respectfully asks the Commission to refrain from pursuing enforcement actions related to the October 24th incident, at least with respect to broadcasters and other EAS Participants who passively retransmitted that EAN in keeping with the rules. [7]

The question remains how to clarify the relevant procedures to prevent similar occurrences in the future, while ensuring the public's access to timely, accurate and consistent EAS alerts.[8] NAB understands that EAS equipment may vary in their processing of EANs with an unclear date or time, or provide users with differing capabilities and setting options. Potential solutions have been discussed on EAS message boards and listservs, such as the periodic dissemination of verification codes as a part of a "red envelope" mechanism, changing the format of EAN date/time stamps

---

[5] *See* 47 C.F.R. §§ 11.33(a)(11), 11.51(m)(2) and (n), and 11.54(a). "EAS Participants" include broadcast stations, cable systems, and Direct Broadcast Satellite Services, among others. *Id*. at § 11.2(d).

[6] Review of the Emergency Alert System, *Notice of Proposed Rulemaking*, EB Docket No. 04-296, 29 FCC Rcd 8123, 8150 (2014) (EAS NPRM).

[7] *See, e.g.*, Reply Comments of Monroe Electronics, Inc., EB Docket No. 04-296 (filed Nov. 19, 2013) at 2-4 (noting the importance of an accurate "time of release" and urging the Commission to require the recognition and processing of all header code elements in an EAS alert).

[8] EAS NPRM at 8150-51.

to include the year, and establishing more uniform standards and settings for EAS boxes, among others. EAS equipment manufacturers also issue periodic software updates, including updates that may address this particular issue. Nevertheless, despite these efforts, improved authentication of EAS messages will persist as a critical issue until a uniform process is clarified.

The technical challenges involved in resolving this problem are complex and require an expertise in EAS equipment design and implementation. While the October 24th case was an isolated incident caused by someone with little familiarity with EAS, the next situation could involve a more purposeful, malicious breach. The potential for mischief is substantial. NAB submits that a joint industry effort can best address the complex authentication issue in a timely manner. The EAS-CAP Industry Group (ECIG) provides an excellent model. The ECIG consisted of a broad coalition of EAS equipment, software and service providers who joined efforts to reach consensus on recommendations that formed the basis of the Commission's rules for EAS message translation. A similar organization could facilitate a consensus protocol for EAS message authentication, subject to Commission approval. NAB would certainly be amenable to participating in such a group.

The Public Notice also seeks comment on industry mechanisms for assessing network integrity and the effectiveness of mitigation measures.[9] While NAB has no direct role in evaluating the security of broadcast networks or equipment, or EAS systems, we do routinely inform and educate radio and television stations regarding

[9] Public Notice at 3.

EAS security, and provide multiple venues for industry dialog and coordination on technical matters.

NAB frequently partners with the Commission to disseminate instructions regarding EAS breaches. For example, NAB supported the Commission's efforts to educate EAS Participants on basic cybersecurity hygiene steps in connection with the unauthorized "Zombie" EAS alert in February 2013. NAB highlighted the Commission's recommendations and forwarded its Public Notice Advisory in an email blast to more than 6,700 industry contacts, and reinforced the message in NAB's biweekly newsletter that reaches more than 7,000 contacts. We undertook similar efforts in relation to the October 24th incident. Later this month, NAB will present a free webcast entitled "Cybersecurity Issues for Broadcasters" that will feature the Chief Counsel for Cybersecurity in the Public Safety and Homeland Security Bureau.

In addition, NAB facilitates radio and television technology committees which consist of leading technologists, engineers and operational executives from each industry. These groups routinely share intelligence regarding the security of broadcast operations and EAS systems. NAB also provides forums for industry discussion of EAS security at our various conventions and conferences. All of these efforts help to increase awareness of cyber risk concerns in the broadcasting industry. Reaching some smaller and rural broadcasters remains a challenge, so we continue to consider additional avenues for keeping these stations informed.

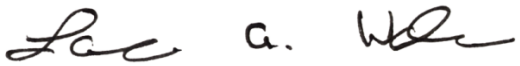
Finally, we observe that broadcasters have strong, market-based incentives to adopt cybersecurity measures to ensure reliable, resilient service. Viewers and listeners rely on broadcasters for uninterrupted live news, entertainment and sports coverage.

More importantly, during weather and other emergencies, broadcasters are America's "First Informers" for life-saving information concerning storm paths, shelter-in-place instructions, evacuation directions and other critical news. Maintaining secure networks and systems is essential to consistent delivery of such important information.

Accordingly, for the reasons described above, NAB specifically requests that the Commission support an industry-driven effort to address EAS message authentication. We look forward to continue working with the Commission to expand awareness of EAS security issues in the broadcasting industry.

Respectfully submitted,

NATIONAL ASSOCIATION OF BROADCASTERS
1771 N Street, NW
Washington, DC 20036
(202) 429-5430



Rick Kaplan
Jerianne Timmerman
Ann West Bobeck
Larry Walke
Kelly Williams

December 5, 2014