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

In the Matter of	)	
	)	
Request for Comment on the Implementation of Emergency Alert System Security Best Practices	)))	DA 14-1628

COMMENTS OF THE NATIONAL ASSOCIATION OF BROADCASTERS

The National Association of Broadcasters (NAB)[1] hereby responds to the Public Notice seeking comment on the recommended best practices for improving the cybersecurity of the Emergency Alert System (EAS) that the Communications, Security, Reliability, and Interoperability Council IV (CSRIC) adopted in June 2014.[2] Broadcasters are aware of cyber-based and other security risks to EAS, and are increasing their responses to minimize those risks. NAB remains committed to supporting these industry efforts through education and the wide dissemination of the CSRIC recommendations.[3]

The Notice seeks comment on industry implementation of the CSRIC recommendations, and the effectiveness of those best practices.[4] As a preliminary matter, NAB notes that it may be too soon to gauge the effectiveness of the best

[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] Public Safety and Homeland Security (PSHS) Bureau Requests Comment on Implementation of Emergency Alert System Security Best Practices, *Public Notice*, DA 14-1628 (*rel*. Nov. 7, 2014) (Notice).
[3] CSRIC IV, Working Group 3, Emergency Alert System, Initial Report (May 2014) (CSRIC EAS Security Report).
[4] Notice at 2.

practices, as these voluntary recommendations were approved by the full CSRIC only six months ago, but not yet explicitly released or published by the Commission. In addition, rapid implementation of the recommendations presents challenges for EAS participants lacking in technical and financial resources, including small or rural entities. For example, a substantial number of radio stations and some smaller television stations do not employ a full-time engineer or operations manager, instead relying on outside consultants who may handle the facilities of multiple stations within a particular region. Moreover, implementing some of the best practices may require IT skills beyond the expertise of typical station staff, such as setting user account restrictions or maintaining firewalls.[5] Identifying and hiring a qualified professional can take time, especially in small and rural markets, and small stations must always carefully budget for any additional costs. The Commission should keep the vastly differing resources of various EAS participants in mind as it considers next steps.

NAB also observes that the CSRIC recommendations will likely be more effective if they remain voluntary, flexible practices. Imposing one-size fits-all cybersecurity mandates or related requirements may cause some participants to only "meet the standard" instead of proactively addressing risks more relevant to their specific operations.[6] Cybersecurity mandates may also inhibit innovation as cyber threats evolve. Mandates necessarily would be based on existing, identified threats and current

[5] *Id*. at 11-12.

[6] Comments of the US Telecom Association, Experience with the Framework for Improving Critical Infrastructure Cybersecurity, U.S. Dept. of Commerce, Docket No. 140721609-4609-01 (Oct. 10, 2014), at 3 (referencing the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (Feb. 12, 2014)).

risk mitigation practices that inevitably will change or become obsolete. Such a backwards-looking approach could serve to open the door to increasingly sophisticated cyber breaches. NAB accordingly urges the Bureau to focus on outreach and increasing awareness among EAS participants of the voluntary best practices contained in the CSRIC EAS Security Report, and allow stakeholders the flexibility to adapt and supplement these practices to suit their facilities.

As a general matter, NAB observes a widespread awareness of EAS security risks in the broadcasting industry. We note that broadcasters were closely involved in the creation of the CSRIC best practices. NAB staff co-chaired the responsible CSRIC working group, which included representatives from multiple radio and television station groups, the Public Broadcasting Service and several state broadcasting associations. As described in our comments on the Bureau's companion inquiry into an improper EAS alert transmitted on October 24, 2014, NAB has repeatedly supported the Commission's efforts to educate EAS participants on cybersecurity measures, beginning almost two years ago with the so-called "Zombie" EAS alert in February 2013.[7] Among more recent efforts, NAB presented a free webcast two weeks ago entitled "Cybersecurity for Broadcasters" that featured the Chief Counsel for Cybersecurity in the Public Safety and Homeland Security Bureau and provided stations with simple, user-friendly guidance on ways to reduce their cyber risks.[8] Senior level engineers and operations managers also share information in several committees and forums facilitated by NAB. EAS

[7] Comments of the National Association of Broadcasters, Request for Comment on the Impact of Unauthorized EAS Alerts, PS Docket No. 14-200 (Dec. 5, 2014), at 4.

[8] NAB's webcast is available at http://www.nab.org/webcast/cyberSecurity-121014/webcast.asp. We will continue to publicize the availability of this webcast to the broadcasting industry.

participants also receive additional advice regarding cybersecurity from other organizations with broadcasting constituencies, such as state broadcasters associations and the Society of Broadcast Engineers. And, unfortunately, EAS participants are further reminded of their risks any time another cyber breach is publicized.

Increasing awareness of both cybersecurity risks and how to address them will prompt action. The Public Notice seeks comment on recurring measures that might help ensure EAS participants maintain an effective security posture.[9] One such measure is for the Commission to provide EAS participants with consistent, recurring reminders and user-friendly guidance. The streamlined best practices attached to the Notice is an excellent first step.[10] Simple, plain language recommendations, like those in the Appendix, are most likely to gain the attention of EAS participants, and not overwhelm smaller entities that have fewer technical resources.

Finally, we observe that, regardless of Commission involvement, radio and television stations have strong, market-based incentives to implement EAS security measures to ensure a consistent, trustworthy EAS system. As the primary source for public warnings and emergency information, Americans rely on broadcasters for uninterrupted coverage of severe weather and other emergency situations. Maintaining a secure, resilient EAS system is essential to this service.

NAB appreciates this opportunity to share our views regarding the CSRIC EAS security recommendations. For the reasons discussed above, we urge the Commission

[9] Notice at 3.

[10] *Id*. at Appendix, “EAS Security Practices.”

to focus on ways to enhance awareness of cyber risks in the EAS ecosystem, and to maintain the CSRIC best practices as flexible recommendations rather than mandates.

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 23, 2014