Brian Hurley
Chief Regulatory Counsel
ACA Connects–America's Communications Association
Seven Parkway Center
Suite 755
Pittsburgh, PA 15220

bhurley@acaconnects.org
(202) 573-6247

April 26, 2023

VIA ECFS

Marlene H. Dortch
Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: PS Docket No. 15-94, *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System*; PS Docket No. 15-91, *Wireless Emergency Alerts*; PS Docket No. 22-329, *Protecting the Nation's Communications Systems From Cybersecurity Threats*

Dear Ms. Dortch:

On April 24, 2023, Jill Canfield and Tamber Ray of NTCA – The Rural Broadband Association, Larry Walke of the National Association of Broadcasters, Brad Greenberg of National Public Radio, and the undersigned of ACA Connects – America's Communications Association met with Danielle Thumann of the Office of Commissioner Brendan Carr. The same individuals met with Hannah Lepow of the Office of Commissioner Geoffrey Starks on April 25, and with Marco Peraza of the Office of Commissioner Nathan Simington on April 26. All meetings were in reference to the Notice of Proposed Rulemaking regarding the security of the Emergency Alert System (EAS) pending in the above-referenced dockets.[1]

Although we strongly support EAS and agree with the FCC that the system must remain reliable and secure, we expressed concern that many of the proposals in the Notice are far too extensive and burdensome for most EAS Participants to implement, especially small and medium-sized entities. In general, the parties are concerned that the proposals in the Notice are not tailored to the size, resources, or capabilities of EAS Participants, especially smaller EAS Participants. We also noted that the FCC relies on fairly scant evidence of cybersecurity

[1] *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, Wireless Emergency Alerts, Protecting the Nation's Communications from Cybersecurity Threats*, Notice of Proposed Rulemaking, PS Docket Nos. 15-94, 15-91, and 22-329 (rel. Oct. 27, 2022) (Notice).

incidents or EAS equipment failures to justify the far-reaching proposals in the Notice.[2] The inherent incentives and existing efforts of communications providers to secure their operations already provide strong motivations for following best practices.

Regarding the specific proposals in the Notice, we noted that the FCC underestimates the resources and expertise required to develop a cybersecurity risk management plan, especially for smaller EAS Participants who will need to hire outside consultants to help create a risk management plan specific to each Participant's needs and capabilities. A "one size fits all" plan would not bolster the security of EAS or EAS Participants' networks as a whole due to the many variables that need to be addressed in any cybersecurity risk management plan. Nor will merely pointing Participants to the comprehensive NIST Cybersecurity Framework for a template plan, without more information from the Commission. While EAS Participants of all sizes take risk management seriously, there is a lack of clarity and guidance in the Notice regarding what may constitute a "sufficient" plan for a small or medium-sized entity. We further explained that most EAS Participants have no in-house cybersecurity expertise, and therefore would likely require extensive – and expensive – assistance from outside consultants to translate the FCC's broad and vague requirements into an actionable plan. Finally, we noted that EAS Participants are regulated entities, and any additional FCC obligation to formally certify as to the sufficiency of one's cybersecurity risk management plan, under threat of FCC enforcement, would demand costly engineering, corporate, and legal review, none of which is reflected in the FCC's cost-benefit analysis of this proposed obligation.[3]

We also noted that Congress designated the Cybersecurity and Infrastructure Agency (CISA) as the lead federal agency regarding cybersecurity incident reporting in the recently enacted Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).[4] CIRCIA provides CISA with wide latitude to develop the rules needed to implement the Act, and directs CISA to share actionable cyber threat information with other federal agencies. Therefore, it would be premature, and potentially duplicative and counter-productive for the Commission to create a cyber-related incident reporting scheme before CISA completes its proceeding. We also noted that certain aspects of the FCC's proposed reporting policies are vague and subjective, and likely to lead to unnecessary over-reporting of cyber-related issues.

The Notice also proposes new policies for the timely repair of faulty EAS equipment and the reporting of EAS equipment failures.[5] The parties agreed with FEMA that such new

[2] Notice at ¶ 4.

[3] Notice at ¶ 31.

[4] Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, Div. Y, § 2246, 136 Stat. 49, 1054 (2022).

[5] *Id*. at ¶¶ 9-12.

obligations are unnecessary and could be unduly burdensome for EAS Participants.[6] We also questioned the purpose of the proposals, given that the FCC plays no role in repairing EAS equipment, and that the time needed to repair EAS equipment is largely beyond the control of EAS Participants.

The parties expressed appreciation for the FCC's attention to EAS, and urged the Commission to pro-actively provide more outreach and education to EAS Participants regarding the maintenance and security of EAS, especially tailored guidance for those entities that may be most vulnerable to cyber threats. We stated our belief that such an approach would be much more effective than merely imposing more regulatory obligations on the entire universe of EAS Participants.

This letter is being filed electronically pursuant to Section 1.1206 of the Commission's rules. Please address to the undersigned any questions regarding this filing.

Sincerely,

Brian Hurley

Cc: Danielle Thumann
Hannah Lepow
Marco Peraza

[6] Comments of the Federal Emergency Management Agency Integrated Public Alert and Warning System Program Office at 2, PS Docket Nos. 15-94, 15-91, and 22-329 (Dec. 16, 2022).