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

In the Matter of	)	
	)	
Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System	)	PS Docket No. 15-94
	)	
Wireless Emergency Alerts	)	PS Docket No. 15-91
	)	
Protecting the Nation's Communications Systems from Cybersecurity Threats	)	PS Docket No. 22-329

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

NTCA–The Rural Broadband Association ("NTCA")[1] hereby submits these comments in response to the Notice of Proposed Rulemaking ("Notice")[2] released by the Federal Communications Commission ("Commission") in the above-captioned proceedings. The Commission requests comment in the Notice on methods to help protect the security of Emergency Alert System ("EAS") equipment. In particular, the Commission proposes to require EAS Participants and Participating Commercial Mobile Service providers (collectively referred to as "Participants") to (1) report compromises of their EAS equipment, including communications systems and services; (2) annually certify to having a cybersecurity risk

[1] NTCA–The Rural Broadband Association represents approximately 850 independent, community-based companies and cooperatives that provide advanced communications services in rural America and more than 400 other firms that support or are themselves engaged in the provision of such services.

[2] *Amendment of the Commission's Rules Regarding the Emergency Alert System,* Notice of Proposed Rulemaking, PS Docket Nos. 15-94, 15-91, and 22-329, FCC 22-82 (rel. Oct. 27, 2022) ("Notice").

management plan in place; (3) ensure the confidentiality, integrity, and availability of their alerting systems; and (4) ensure only valid alerts are displayed on consumer devices.[3]

NTCA supports the Commission's goal of helping to ensure the security of emergency alerts; however, NTCA encourages the Commission to avoid developing incident reporting rules that conflict with those being developed by the Cybersecurity and Infrastructure Security Agency ("CISA") pursuant to Congress' directive in the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"). NTCA also urges the Commission not to impose unclear, subjective cybersecurity standards that would likely place smaller Participants at a much higher risk of falling short of such standards. NTCA further encourages the Commission to conduct further review of the cost to Participants of carrying out the actions proposed in the Notice, including the cost of purchasing new or upgraded equipment that would be necessary to fulfill the proposed security requirements.

I. The Commission Should Avoid Duplicating or Adding to Reporting Requirements Established by CIRCIA.

The Notice proposes to require Participants to report any incident of unauthorized access "to any of their communications systems or services that potentially could affect their provision of EAS" within 72 hours of when the Participant "knew or should have known" the incident occurred.[4] Proposing rules that would require Participants to report instances of unauthorized access of their communications systems is premature. CIRCIA directed CISA to develop rules requiring critical infrastructure entities, which include communications providers, to report cyber incidents to CISA. CIRCIA also directed CISA to identify the entities that will be required to

[3] Notice at ¶ 1.

[4] *Id*. at ¶¶ 13-14.

submit cyber incident reports, how those reports will be submitted and the content of the reports. Pursuant to this directive, CIRCIA instructed CISA to publish a Notice of Proposed Rulemaking by March 2024 and to consult with government and private stakeholders prior to issuing cyber incident reporting rules.[5]

CIRCIA further instructs CISA to "rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures" based on the information contained in the incident report.[6] Accordingly, to the extent CISA adopts rules requiring communications providers to report cyber incidents, the Commission will have the ability to receive relevant information from CISA about such incidents. As a result, the reporting requirement proposed in the Notice is premature and has the potential to duplicate at best or, at worst, conflict with CIRCIA reporting requirements. At a minimum, the Commission should avoid creating new reporting requirements involving unauthorized access to communications equipment until CISA has completed the cyber incident rulemaking pursuant to CIRCIA and the Commission can then more clearly establish what, if any, gaps need to be filled.

Additionally, the Commission's proposal to require Participants to "report any incident of unauthorized access to any aspects of an EAS Participant's communications systems and services that *potentially* could affect their provision of EAS"[7] lacks clarity, conflicts with CIRCIA, and would take important time away from Participants and the Commission in preparing and reviewing reports even when security measures were successful and harms did not develop. Similarly, the

[5] Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), Public Law 117-103, Div. Y (2022) (to be codified at 6 U.S.C. 681-681g) at sec. 2242(b)(1).

[6] CIRCIA at sec. 2245(a)(2)(A).

[7] Notice at ¶ 14 (emphasis added).

Commission's proposed standard of "knew or should have known" of any unauthorized access is vague and highly subjective. Whether an intrusion has the potential to affect provision of EAS (even in instances where EAS alerts were not affected) or whether an entity should have known of unauthorized access to equipment would likely look different when viewed after the fact and could easily vary from one entity to the next in part due to the entity's staffing levels and technical knowledge and capabilities. Thus, adopting rules requiring reports to be filed when there is the "potential" for unauthorized access to EAS equipment and when Participants "should have known" of any unauthorized access would create a nearly immeasurable reporting threshold and would almost inevitably put small entities at greater risk of violating the Commission's rules due to small entities' limited staffing and financial capabilities.

Finally, even if reports are nonetheless required in advance of CISA's implementation of cyber incident reporting rules pursuant to CIRCIA, NTCA encourages the Commission not to require Participants to report incidents that take place on third party providers' systems or products such as firewalls or Virtual Private Networks[8] and to refrain from modifying existing EAS outage reporting requirements until after CISA has adopted rules pursuant to CIRCIA. When considering incident reporting rules, the Commission should also be mindful of the sensitive nature of Participants' equipment and operations. In particular, given the Notice's proposal to require Participants to file detailed information regarding any compromise of either their EAS equipment or other network equipment in NORS, the Commission should be mindful of the ability of Federal,

[8] Smaller providers commonly utilize managed service providers for firewall and VPNs. As a result, these providers will likely know very little, if anything, regarding incidents that take place on these types of equipment or services – especially if such incidents do not result in any interruption of EAS or other services offered by the provider - as they are outside the provider's domain. As a result, the provider would be unable to provide information in an incident report that could help prevent a similar incident from occurring.

state, Tribal nation, territorial, and District of Columbia agencies to obtain access to information filed by providers in NORS.[9] Congress has already recognized the importance of protecting the confidentiality of information submitted in cyber incident reports pursuant to CIRCIA.[10] The information proposed to be submitted to the Commission in the Notice is no less important to protect.

II. Cyber Risk Management Practices Should Not Place Small Participants at a Disadvantage.

The Notice proposes to require Participants to certify annually that they have "created, updated, and implemented a cybersecurity risk management plan."[11] NTCA recognizes the importance of a cybersecurity risk management plan as part of a company's overall cybersecurity practice; however, guidelines for risk management plans, including the NIST CSF, are designed to be flexible and scalable to meet company needs, and not prescriptive requirements. The Commission's proposal to hold Participants accountable for "negligent security practices" or a "failure to sufficiently develop or implement" a risk management plan is very subjective and could place small Participants at a significant disadvantage as their security practices could appear negligent and their risk management plan could appear "insufficient" when compared to a larger Participant with more technical experts and financial capabilities. Furthermore, a Commission finding of "negligence" or "failure to sufficiently develop or implement" a risk management plan could have significant economic consequences and repercussions on any Participant.

[9] *See Amendment to Part 4 of the Commission's Rules Concerning Disruptions to Communications*, PS Docket No. 15-80, Second Report and Order, 36 FCC Rcd 6136 (March 18, 2021).

[10] *See generally* CIRCIA at sec. 2245(b).

[11] Notice at ¶ 23.

NTCA also encourages the Commission to more fully detail and seek further comment on the Notice's proposal to require Participants to identify "the cyber risks that they face, the controls they use to mitigate those risks, and how they ensure that these controls are applied effectively to their operations."[12] This is especially necessary given the Commission's proposal to treat a Participant's "failure to sufficiently develop or implement their plan" as a violation of the Commission's rules.[13] The NIST CSF, for example, which is intended to be adapted to the needs and capabilities of individual companies, recognizes that "the variety of ways in which the Framework can be used by an organization means that phrases like 'compliance with the Framework' can be confusing and mean something different to various stakeholders."[14] Presumably, there will be some threshold of insufficient development or implementation below which a rule violation would be found. The Commission should seek comment on a proposed threshold in order to obtain informed feedback from the community then, based on the feedback received, offer clear guidance to Participants in lieu of vague measures of "sufficiency."

III. The Commission Can Ensure Operational Readiness of EAS by Identifying Barriers and Working with Participants to Address Them.

In response to the Commission's request for comment on how to better promote the operational readiness of EAS equipment, including the barriers that prevent equipment from being repaired promptly and how the Commission can help remove those barriers,[15] NTCA notes that the shipping time, distance between locations and the availability (or unavailability) of parts for

[12] *Id.*

[13] *Id.* at ¶ 30.

[14] NIST Framework for Improving Critical Infrastructure, v. 1.1 (Apr. 16, 2018), p. vi, available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[15] Notice at ¶ 10.

older equipment can all contribute to delays in repairing EAS equipment. Additionally, the Notice presumes a "one-time cost" for Wireless Emergency Alert ("WEA") participants to update the "standards and software" necessary to comply with the security requirements proposed in the Notice.[16] The estimated cost, however, also presumes all WEA participants utilize the same equipment and software, including the software version, and that the software will only need to be updated once to meet the proposed security requirements.

Subjecting Participants to costly upgrades, time-consuming and possibly duplicative reporting requirements as well as poorly defined and subjective compliance standards will likely create more barriers to the operational readiness of EAS equipment. Instead, NTCA encourages the Commission to identify methods of assisting with the cost and other associated logistics of purchasing equipment and software that would help secure EAS alerts while also addressing the delays commonly encountered in acquiring and installing communications equipment and software of any type.[17]

IV. Conclusion

Requiring Participants to adhere to subjective requirements will be more likely to cause confusion and damage to Participants than add more security to EAS alerts. Likewise, subjecting Participants to duplicative reporting requirements, which as proposed could result in sensitive information about equipment locations being widely available, does little to improve the security of EAS alerts and instead would be time consuming and costly to Participants while also drawing

[16] *Id.* at ¶ 40.

[17] *See, e.g.*, Fact Sheet: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China, The White House, Aug. 9, 2022 (available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/).

critical time and attention away from restoring communications and resolving the cause of the incident. Accordingly, NTCA encourages the Commission not to adopt any reporting requirements prior to CISA's implementation of CIRCIA or to require adherence to subjective risk management plans that could put small Participants at risk of being found in violation of the Commission's rules.

Respectfully submitted,

By: */s/ Michael Romano*
Michael Romano
Tamber Ray

4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203
(703) 351-2000