Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

COMMENTS OF NATIVE PUBLIC MEDIA

Native Public Media ("NPM") respectfully submits these comments in response to the Federal Communications Commission's ("FCC" or "Commission") Notice of Proposed Rulemaking ("NPRM") in the above-captioned proceedings.[1]

Founded in 2004, NPM is a non-profit national organization whose mission is to encourage the expansion and strengthening of Native media through platforms that are community-based, local, and democratic. NPM, as a national center, provides leadership, centralized resources, and strategic and coordinated approaches to strengthen the Native Broadcast System successfully. These services include broadcast licensing guidance, FCC and Corporation for Public Broadcasting compliance, station operations guidance, legal guidance, broadcast leadership training and education, and telecommunications and communications policymaking.

[1] Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System; Wireless Emergency Alerts; Protecting the Nation's Communications Systems from Cybersecurity Threats, PS Docket Nos. 15-94, 15-91, and 22-329, Notice of Proposed Rulemaking, FCC 22-82 (Oct. 27, 2022); Federal Communications Commission, Emergency Alert System; Wireless Emergency Alerts; Protecting the Nation's Communications Systems from Cybersecurity Threats, Proposed Rule, 87 FR 71539 (Nov. 23, 2022).

Over the past 18 years, NPM has grown into a network of 57 Native radio stations and 4 television stations. Native stations play a vitally important role in the communities they serve. Native stations serve as an essential source of news, deliver critically important health information, provide a forum for discussion and debate around the issues that affect their communities, broadcast life-saving information in times of emergencies, air extensive cultural content, promote language preservation, and provide jobs as part of the local economy.

Native stations are small staffed, located in remote, rural areas with limited access to professional services including legal, engineering, and other support. The organizational capacity and budgets are taxed by the cost of doing business on Tribal reservations miles away in proximity to service and retail outlets.

NPM strongly supports the Commission efforts to ensure that all radio and television licensees remain vigilant and proactive in securing their Emergency Alert System ("EAS") equipment from cyberattacks. However, the simple reality is that NPM station members have neither the resources, nor the expertise to shoulder that responsibility properly. Rather, it is the Commission itself that must take on this responsibility by providing both the necessary resources and the required expertise to NPM members and other small entity licensees who already grapple with limited technical and staff resources, as well as daunting budgetary constraints.

I. NPM Members Have Neither the Resources Nor the Expertise to Develop and Implement Cybersecurity Risk Management Plans

The Commission proposes to require each broadcast licensee to annually certify that it has "created, annually updated, and implemented a cybersecurity risk management plan"[2] and suggests that licensees can structure their plans to follow established risk management frameworks such as the National Institute of Standards and Technology ("NIST") Risk

[2] Proposed 11.35(d)(1), NPRM at p. 26.

Management Framework or the NIST Cybersecurity Framework.[3] More specifically, the Commission proposes that each cybersecurity risk management plan generally include "security controls sufficient to ensure the confidentiality, integrity, and availability (CIA) of the EAS,"[4] and specifically include "measures that address changing default passwords prior to operation, installing security updates in a timely manner, securing equipment behind properly configured firewalls or using other segmentation practices, requiring multifactor authentication where applicable, addressing the replacement of end-of-life equipment, and wiping, clearing, or encrypting user information before disposing of old devices."[5]

Although the Commission estimates that it will "on average, require 10 hours annually to initially draft a plan and then update the plan and submit [a] certification annually,"[6] NPM strongly believes that the Commission has significantly underestimated the effort that will be required for small entity broadcasters to develop the expertise necessary for such a project. More realistically, most small entity licensees will need to identify and rely on outside expert consultants to assist with the daunting task of developing and implementing a NIST-compliant cybersecurity risk management plan which will likely cost tens of thousands of dollars.[7]

Moreover, developing and implementing a cybersecurity risk management plan is not a one-off expense, but requires sustained on-going expertise and vigilance. The techniques used by cyber criminals are ever-changing, as are the methods and technology used to counter cyberattacks. While changing default password codes and installing firewalls might have been

[3] NPRM at ¶ 24.
[4] NPRM at ¶ 25.
[5] *Id*.
[6] NPRM at ¶ 32. NPM notes that the Commission does not provide any basis for its determination that it will take an average of 10 hours annually for each licensee to draft and update a cybersecurity risk management plan.
[7] *See*, *e.g.*, https://www.goldskysecurity.com/estimated-costs-associated-with-nist-800-53-and-nist-800-171-security-risk-assessments/ (cost of developing in-house expertise simply to conduct a security risk assessment estimated at $30,000 - $35,000; cost of using an expert consultant estimated at $10,000 - $15,000).

enough to prevent the 2013 "zombie attack" incident described in the NPRM,[8] 2013 cyberattacks techniques are now a distant memory. This is especially true given that the Commission recently revised its EAS rules to require that broadcasters prioritize use of Internet-based Common Alerting Protocol (CAP) formatted alerts, thereby rendering EAS alerts even more vulnerable to ever-increasingly sophisticated IP-based cyberattacks.[9]

The integrity of the EAS system is ultimately an issue of national security.[10] If the Commission determines to impose a cybersecurity risk management plan requirement on broadcast licensees, the FCC itself must make expert resources available to assist small entity broadcasters in this effort for two reasons. First, the costs would otherwise be prohibitive for already struggling operators and second, leveraging the expertise of the Federal government would ensure that cybersecurity risk management plans are properly developed and implemented.

In a separate Commission proceeding related to whether the Commission should permit E-Rate funds to be used for network security services such as advanced or next-generation firewalls and services, the Commission recently cited a U.S. Government Accounting Office ("GAO") finding that Federal coordination is needed to enhance K-12 cybersecurity.[11] Similarly, Federal coordination is needed to enhance EAS security. Borrowing from the GAO report on K-12 cybersecurity, such coordination should include a collaborative mechanism. A government coordinating council, for example, could coordinate cybersecurity efforts among

[8] NPRM at ¶ 4.
[9] Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, PS Docket No. 15-94, Report and Order, FCC 22-75 (Sept. 30, 2022); Federal Communications Commission, The Emergency Alert System, 87 FR 67808 (Nov. 10, 2022).
[10] The primary purpose of the EAS is to provide the President of the United States with the capacity to provide the Nation with immediate communication and information during periods of national emergency. NPRM at ¶ 2.
[11] Wireline Competition Bureau Seeks Comment on Requests to Allow the Use of E-Rate Funds for Advanced or Next Generation Firewalls and Other Network Security Services, WC Docket No. 13-184, Public Notice, DA 22-1315 (Dec. 14, 2022); GAO, Critical Infrastructure Protection Additional Federal Coordination is Needed to Enhance K-12 Cybersecurity (2022), https://www.gao.gov/assets/gao-23-105480.pdf.

federal agencies (*e.g.*, the FCC, the Federal Emergency Management Agency, and the Cybersecurity and Infrastructure Security Agency) to provide broadcasters with technical guidance and cybersecurity-related products and services that address both current and future EAS cyber threats.

II. Incident Notification

The Commission also proposes to require that broadcasters report any incident of unauthorized EAS access to the Commission within 72 hours.[12] This notification requirement would not only include a description of the unauthorized EAS access but also "a description of the vulnerabilities exploited and the techniques used to access the device, identifying information for each actor responsible for the incident."[13] Although NPM supports the proposed implementation of an expedited notification procedure for any incident of unauthorized EAS access, this notification should only require broadcast licensees to provide the Commission with information that is in fact known by the licensee at the time of the notification, without requiring further assessment or investigation regarding who was responsible for the incident. As discussed above, NPM members and other small entity broadcasters simply do not have the expertise or resources to conduct cybersecurity investigations, let alone within a 72-hour window. Instead, the Commission should use these initial expedited notifications to trigger an assessment by the Commission's experts of what further investigation is necessary and appropriate. The Commission's same resources should both support broadcasters in their development and

[12] NPRM at ¶ 13.
[13] Proposed 11.45(c), NPRM at p. 27.

implementation of cybersecurity risk management plans, and to investigate and address any reported cyberattacks.

Respectfully submitted,

NATIVE PUBLIC MEDIA

By: Loris Taylor
Loris Ann Taylor
President
P.O. Box 3955
Flagstaff, AZ 86003
(928) 853-2430

By: _____
Brad C. Deutsch
Melodie A. Virtue
FOSTER GARVEY P.C.
1000 Potomac St., N.W. Suite 200
Washington, DC 20007
(202) 965-7880
Its Attorneys

Dated: December 23, 2022