Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 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 Alerts	)	PS Docket No. 15-91
	)	
Protecting the Nation's Communications Systems from Cybersecurity Threats	))	PS Docket No. 22-329

To: The Commission

JOINT COMMENTS OF THE
STATE BROADCASTERS ASSOCIATIONS

Scott R. Flick
Lauren Lynch Flick

Pillsbury Winthrop Shaw Pittman LLP
1200 Seventeenth Street, NW
Washington, DC 20036
(202) 663-8000

Their Attorneys in This Matter

December 23, 2022

TABLE OF CONTENTS

Page

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 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 Alerts	))	PS Docket No. 15-91
	)	
Protecting the Nation's Communications Systems from Cybersecurity Threats	))	PS Docket No. 22-329

To: The Commission

JOINT COMMENTS OF THE STATE BROADCASTERS ASSOCIATIONS

The Alabama Broadcasters Association, Alaska Broadcasters Association, Arizona Broadcasters Association, Arkansas Broadcasters Association, California Broadcasters Association, Colorado Broadcasters Association, Connecticut Broadcasters Association, Florida Association of Broadcasters, Georgia Association of Broadcasters, Hawaii Association of Broadcasters, Idaho State Broadcasters Association, Illinois Broadcasters Association, Indiana Broadcasters Association, Iowa Broadcasters Association, Kansas Association of Broadcasters, Kentucky Broadcasters Association, Louisiana Association of Broadcasters, Maine Association of Broadcasters, MD/DC/DE Broadcasters Association, Massachusetts Broadcasters Association, Michigan Association of Broadcasters, Minnesota Broadcasters Association, Mississippi Association of Broadcasters, Missouri Broadcasters Association, Montana Broadcasters

Association, Nebraska Broadcasters Association, Nevada Broadcasters Association, New Hampshire Association of Broadcasters, New Jersey Broadcasters Association, New Mexico Broadcasters Association, The New York State Broadcasters Association, Inc., North Carolina Association of Broadcasters, North Dakota Broadcasters Association, Ohio Association of Broadcasters, Oklahoma Association of Broadcasters, Oregon Association of Broadcasters, Pennsylvania Association of Broadcasters, Radio Broadcasters Association of Puerto Rico, Rhode Island Broadcasters Association, South Carolina Broadcasters Association, South Dakota Broadcasters Association, Tennessee Association of Broadcasters, Texas Association of Broadcasters, Utah Broadcasters Association, Vermont Association of Broadcasters, Virginia Association of Broadcasters, Washington State Association of Broadcasters, West Virginia Broadcasters Association, Wisconsin Broadcasters Association, and Wyoming Association of Broadcasters (collectively, the "State Associations"), by their attorneys in this matter, hereby file these Joint Comments in response to the Commission's Notice of Proposed Rulemaking released October 27, 2022 in the above-captioned proceeding.[1]

INTRODUCTION AND SUMMARY

The Emergency Alert System ("EAS") and its predecessors have been a success story of cooperation between the private and public sectors to enable the dissemination of emergency messages to the American public since the 1950s. As evidenced by the system's one-time name, the Emergency Broadcast System, broadcasters have been at the center of this partnership since the very beginning. Broadcasters dedicate substantial resources to their role in the EAS by conducting weekly, monthly and periodic nationwide tests of the system, all in preparation for

[1] *See Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, et al.,* Notice of Proposed Rulemaking, PS Docket No. 15-94, FCC 22-82 ("*NPRM*") (rel. Oct. 27, 2022).

carrying the one alert that has never been issued, the Presidential Alert message, recently renamed the National Emergency Message.[2] Broadcasters also voluntarily transmit untold thousands of other messages originated by the National Weather Service, the Federal Emergency Management Agency, and myriad state, local, and Tribal civil and law enforcement agencies, covering a wide array of weather emergencies, Amber Alerts, and other localized emergency messages far removed from — but for local communities no less important than — the Presidential Alert for which the system was originally designed.

Broadcasters also serve in voluntary capacities as State Emergency Communications Committee ("SECC") Chairs and members, working countless uncompensated hours crafting and obtaining FCC approval of State Plans addressing the operation of the EAS in their respective states, answering EAS Participants' questions, interfacing with state and local emergency managers and other EAS stakeholders, and generally managing their state's EAS on a day-to-day basis. Broadcasters also provided volunteer members to the former National Advisory Committee ("NAC"), which allowed for dialog and information sharing between the FCC and EAS Participants to improve the operation and effectiveness of the system, and now are among the members of the Communications Security, Reliability and Interoperability Council ("CSRIC") and its various working groups to facilitate the operation and ongoing evolution of the system.

Thus, broadcasters have historically invested and continue to invest considerable time, effort, and financial resources in maintaining, operating and contributing to the success of the EAS. However, the system has evolved considerably over time and incorporates many other players besides broadcasters who both add new redundancies and strengths to the system and

[2] *See Amendment of the Commission's Rules Regarding the Emergency Alert System*, Report and Order, Report and Order, PS Docket 15-94, FCC 22-75 (rel. Sept. 30, 2022).

introduce new vulnerabilities. While it is likely that the EAS will continue to evolve over time, changing in some ways the manner in which broadcasters participate in it, the approach set out by the FCC in the *NPRM* for the latest round of "enhancements" creates an enormous unfunded mandate that exponentially increases the financial, time and liability burdens on EAS Participants to an extent that broadcasters cannot simply absorb. As broadcasters have repeatedly reminded the FCC in connection with its assessment of annual regulatory fees, broadcasters do not have a subscriber base onto which they can pass costs, such as fees for upgrades that EAS equipment manufacturers could implement to improve security of the system, or expenses to hire additional station personnel and third-party services to help them implement, monitor and update cumbersome cybersecurity risk and incident response plans. The *NPRM* proposes to couple this dramatic increase in cost and human capital with a harsh enforcement stance that hardly seems appropriate given the cooperative nature of the EAS and particularly broadcasters' downstream role in it. Taken together, the proposals set forth in the *NPRM* disincentivize broadcaster participation beyond the bare minimum required, particularly for rural market broadcasters, and therefore risk undermining the EAS entirely.

The FCC proposes to require EAS Participants to report to the FCC when their EAS equipment is out of order, even though there is little the FCC can do with that information. The FCC also proposes to require EAS Participants to report on unauthorized access to any station system that might affect their provision of EAS, but does not acknowledge the burdens and costs of setting up the surveillance and monitoring necessary to comply with such a reporting requirement. Finally, the FCC proposes to require EAS Participants to draft, implement and certify to having sophisticated cybersecurity plans, all at considerable cost and with little guidance.

Yet, there are many simpler — and potentially more effective — steps that the FCC could take that would enhance the security and function of the EAS, such as working with equipment manufacturers to incorporate cybersecurity measures into the hardware and software they provide and encouraging the use of more secure alternatives to the public Internet. Thus, rather than requiring broadcasters to file more reports and take on the primary responsibility for continuous threat awareness and monitoring, the FCC should partner with the industry by reestablishing an ongoing dialogue with the broadcaster community and broader EAS ecosystem to increase mutual understanding of the issues the FCC is attempting to address, and provide training and informational resources to broadcasters to help achieve those goals. The FCC should also seek financial resources from Congress, the Department of Homeland Security, the National Telecommunications and Information Administration and other sources to help broadcasters implement any desired software, hardware and cybersecurity upgrades, as well as to bolster equipment manufacturers in offering appropriate products to achieve the FCC's goals. Consistent with the above and in recognition of the longstanding partnership with broadcasters that has made the development and operation of the current EAS possible, the FCC should not adopt the enforcement stance set forth in the *NPRM*.

I. Replacing the Current 60-Day Repair Period for EAS Equipment and Requiring Reporting of Equipment Operational Status Impose Additional Burdens on Broadcasters Without Clear Benefits

In the *NPRM*, the FCC asks for comment on proposals that would require broadcasters to report to the FCC when their EAS equipment is out of order,[3] as well as to meet a nebulous

[3] It is noted that at some points in the *NPRM*, the FCC speaks in terms of "equipment failures" and at others in terms of "defective" EAS equipment or equipment "defects." *See, e.g.*, *NPRM* at ¶¶ 9, 11. The State Associations assume that the FCC is using these terms interchangeably to refer to equipment that is not in proper working order whether the cause is a manufacturing defect or some other technical and/or physical malfunction or damage. If that is not the case, the Commission should clarify that fact and request further comments on the subject.

standard requiring “prompt” and “reasonably diligent” repair of EAS equipment. The Commission inquires as to whether these changes will assist the “situational awareness” of the FCC and Alert Originators, but does not ask the more fundamental questions of whether the proposals will assist broadcasters in getting their equipment back into operation any quicker and result in better transmission of EAS messages. It seems unlikely that an Alert Originator would forego activating the EAS because one or two radio stations throughout the alert area are off the air or have suffered an equipment failure of some sort. The redundancy built into the system, specifically that other area radio, television, cable, and wireless operators are likely carrying the same message at the same time, would make taking such a step unnecessary, especially if broadcasters are also carrying breaking news coverage of the event, which is frequently the case.

Similarly, with the loss of most local FCC field offices, it is unlikely that the Commission could productively react to equipment failure reporting by providing broadcasters in such circumstances with loaner equipment or assistance in installing replacement equipment, and thereby hasten a station’s resumption of EAS capability. Given that, it seems the proposed notification requirement would principally be used to fine broadcasters and encumber license renewals rather than improve the EAS system.

A. The 2021 Nationwide Periodic Test Was a Success

The FCC posits that more regulation of broadcasters’ repair of EAS equipment is necessary because in the August 11, 2021 nationwide periodic test, out of more than 19,000 EAS Participants, fewer than 1,000 reported an issue with either receiving or retransmitting the test due to an equipment performance issue.[4] These numbers are for all EAS Participants, not just broadcasters. The Commission's report on the 2021 test does not identify the number of *broadcast* EAS Participants that reported equipment performance issues, and that information apparently has not been shared with SECC Chairs, either. Thus, the SECC Chairs cannot help identify and address any issues that may recur in the next test, and the State Associations cannot assess the level of success achieved by broadcaster EAS Participants in their state in the last test. Nevertheless, the State Associations wish to point out that the numbers the FCC references reflect an overall success rate of **over 95% for individual EAS Participants**, and given the many redundancies built into the system, an even higher success rate in one or more EAS alerts being accessible to the public even accounting for individual equipment failures. The success of the system's design is its redundancy, as opposed to relying on the unrealistic expectation that all equipment and connections between them will be flawless. While perfect performance may be the hoped-for outcome and a laudable goal, the August 2021 test must be seen as a success with respect to equipment readiness, not the dismal failure the *NPRM* makes it out to be.

B. The Current 60-Day Repair Period Provides Needed Certainty and Works Well

Currently, under Section 11.35(b) of the Commission's Rules, a broadcaster may take its EAS equipment out of service for repairs for a period of up to 60 days without prior FCC authorization.[5] The Commission asks whether it should eliminate this readily understood and administrable rule of long standing and impose instead a vague requirement that repairs be

[4] *NPRM* at ¶ 9, n. 45. The FEMA IPAWS Program Office in its comments in this proceeding states that the incidence of equipment failure over the past five years has been less than 0.5%, putting the success rate at 99.5% or better. *See* Comments of the Federal Emergency Management (FEMA) Integrated Public Alert and Warning System (IPAWS) Program Office, PS Docket No. 15-94 (December 16, 2022) at 2.

[5] 47 C.F.R. § 11.35(b).

conducted "promptly and with reasonable diligence."[6] The impression one is left with in reading the paragraph of the *NPRM* where the Commission asks this question is that the Commission does not consider a 60-day repair period to be reasonably prompt and diligent. Yet, the *NPRM* a paragraph earlier asks what steps are needed to repair the equipment and how long those steps take, indicating that the Commission does not have any other rational timeframe by which to measure compliance, whether it be more or less than 60 days.

In the State Associations' experience, most EAS equipment is not field repairable. In general, if a station's EAS equipment is not functioning properly, the station must have an engineer remove the equipment and ship it back to the manufacturer for repair. Upon receipt of the equipment back from the manufacturer, an engineer must reinstall and test it before it is operational again. The station's chief operator, who is often the owner or an employee without specific engineering training, would not likely attempt to diagnose the failure, disconnect the equipment to send it back to the manufacturer or reinstall the equipment once repaired and returned, because the station's entire audio output is usually fed through the box and an error on that individual's part could leave the station off the air entirely (devastating to the station and hardly helpful to the public during an emergency). While a large group owner of multiple stations may have the engineering resources for these tasks on its staff, and perhaps even some spare EAS equipment available for use while malfunctioning equipment is out for repair, many single station or small group owners, and especially those in small markets and rural locations, will not.

Particularly for a small market broadcast station, each of the steps identified above can create considerable delay. In the event of equipment malfunction, the station would contact a

[6] *NPRM* at ¶ 10.

contract engineer and schedule a visit to the station to undertake the work of confirming the nature of the failure, disconnecting the EAS equipment, and packing and shipping it back to the manufacturer. The contract engineer may have to travel a considerable distance and/or fit this EAS work in around full-time work for another broadcaster. Once the equipment is removed, packed and shipped, the turnaround time to receive it back from the manufacturer is out of the broadcaster's control and depends on the backlog at the manufacturer and any supply chain shortages that the manufacturer is experiencing at the time. Then, once the repaired equipment is returned by the manufacturer, the station must repeat the process of reaching out to a contract engineer to schedule the reinstallation of the equipment, including necessary travel time, before the station's EAS will be operational again.

Given the myriad different circumstances that can apply to each equipment malfunction, as well as each broadcast station's situation and location, a nebulous standard of "prompt" and "diligent" simply invites confusion and post hoc enforcement that is completely inappropriate in a cooperative government and industry program. Indeed, the rural broadcaster, familiar with the process of securing a contract engineer and the FCC's long-standing 60-day rule, but not having read the tone of this paragraph in the *NPRM*, might well reasonably conclude that more than 60 days is both prompt and diligent under his/her circumstances. In contrast, the current 60-day repair period is a clear and easily understood rule and does not take broadcaster time and attention away from working on the logistics of the needed repair to send a notification which will likely have no real-world impact on the broadcaster's ability to return the equipment to service any sooner.

II. Reporting Events of Unauthorized Access to All Station "Communications Systems and Services" Is Overbroad and Burdensome

The Commission also asks whether it should expand its requirement that stations report having sent a false EAS message to also include requiring stations to report any "remote or local access to EAS equipment, communications systems, or services by an individual or other entity that does not have permission to access the equipment or exceeds their authorized access."[7] This reporting obligation would cover not only the EAS equipment, but "any aspects of an EAS Participant's communications systems and services that potentially could affect their provision of EAS,"[8] including all "infrastructure that serves to prevent unauthorized access to EAS equipment, including firewalls and Virtual Private Networks."[9]

The FCC suggests that these reports should be made via the Commission's Network Outage Reporting System ("NORS"), a system that broadcasters do not even use, and that they be made within 72 hours, or perhaps even sooner, from when the broadcaster "knew or should have known" that the incident of unauthorized access has occurred.[10] The FCC states that it expects this reporting requirement to be no more difficult, costly or time-consuming than the existing false EAS message reporting requirement, which only involves sending an email to the FCC within 24 hours of discovering having actually sent a false alert.[11] The FCC justifies the imposition of this new requirement because the FCC "could" use the information from the reports

[7] *NPRM* at ¶ 18.
[8] *NPRM* at ¶ 14.
[9] *NPRM* at ¶ 14.
[10] *NPRM* at ¶ 18.
[11] *NPRM* at ¶ 17.

to help remediate the breach or better secure the system, but does not explain how this would occur or make any commitments to do so.[12]

As noted above with regard to the EAS equipment operational status reporting proposal, the FCC does not have teams of cybersecurity specialists at the ready to deploy anywhere in the country upon learning of a breach at a broadcast station. Thus, the reporting requirement is unlikely to bring resources to the broadcaster's doorstep to assist in addressing the unauthorized access. It is also unlikely that the FCC could or would take the EAS system offline in a particular state upon receiving a report. So, the reporting of such an event would not likely lead to a faster remediation of the issue or dissuade an Alert Originator from issuing an alert in the case of an emergency. Thus, it again seems that the FCC is proposing to add yet another obligation to broadcasters' plates that will not assist in providing EAS alerts or making those alerts more reliable.

Moreover, the obligations placed on broadcasters under the intrusion reporting proposal are much greater than those involved in the EAS equipment readiness reporting proposal. The most likely way a broadcaster would learn it has experienced unauthorized access of its EAS equipment is to have sent an unintended EAS message. Absent having sent such a message, the only way a broadcaster could comply with the proposed reporting requirement is constant monitoring of every aspect of station operations[13] and having sufficient training and experience to ferret out the signs of an intrusion.

[12] *NPRM* at ¶ 16.

[13] While the focus of the *NPRM* is cybersecurity, the definition of unauthorized access would seem to encompass means other than just those involving breaching VPNs and firewalls that have been tried in the past to gain access to EAS equipment.

The reporting requirement presupposes that the reporting entity will have a variety and level of skills and training that may greatly exceed those that many, particularly smaller, broadcasters possess. For example, the proposed content of the notification, which includes providing "a description of the vulnerabilities exploited and the techniques used to access the device," and "identifying information for each actor responsible for the incident"[14] are fairly sophisticated and may never be known for any given incident, even where fairly sophisticated cybersecurity capabilities are available.

The *NPRM* also does not provide any guidance to EAS Participants about how to set up system surveillance and monitor in ways that the FCC would find to be satisfactory or even indicate which systems at a broadcast station should be covered by such surveillance and monitoring. For example, it is not clear whether the mere receipt of a phishing attempt email by station personnel is sufficient to trigger a report to the FCC. Nor does the *NPRM* take those financial and time expenditures into account when calculating the cost of compliance. Rather, the *NPRM* attempts to characterize these precursors to the reporting requirement as nothing more than ordinary activities already engaged in by broadcasters. While some broadcasters will have very sophisticated systems and expertise on staff, others may be relying on off the shelf solutions and only engage more sophisticated technical assistance on an as needed basis. Both types of entities (and everyone in between) require guidance from the FCC as to what types and levels of surveillance will be deemed acceptable by the FCC.

Moreover, the proposed timeframe for making the report, within 72 hours of when the station knew *or should have known* of the intrusion, appears to be another opening for "gotcha"

[14] *NPRM* at ¶ 19.

style enforcement that merely encourages stations that belatedly find out about an intrusion to keep that information to themselves rather than notify the FCC of what might be a systemic problem that could be fixed before it strikes other stations. This is precisely how ***not*** to design a notification system aimed at finding and correcting fixable flaws. Headlines are legion of situations where intrusions have gone undetected for long periods of time before finally being uncovered. For example, the intrusion at the bottom of SolarWinds, arguably the most infamous of all cybersecurity breaches, which involved thousands of companies and government agencies, including the Department of Homeland Security (which should be well versed in all things cybersecurity), occurred more than a year before the existence of the malicious code was discovered.[15] Even then, entities like Microsoft reportedly only discovered their own involvement by seeing signs of the malicious code in their customers' systems.[16] Here again, broadcasters would hope their long-time partner agency, the FCC, would be working with them and providing support and funding to their efforts to meet any new obligations under the Cyber Incident Reporting for Critical Infrastructure Act of 2022, rather than using its life and death hold over broadcasters' licenses to mete out penalties for falling short of unrealistic expectations thrust upon the industry without sufficient support.

III. The *NPRM*'s Proposals Around the Development, Implementation and Certification of Cybersecurity Plans Are Similarly Overbroad and Burdensome

Finally, the *NPRM* proposes to require EAS Participants to draft, implement and certify to the FCC that they have created a cybersecurity plan that covers, again, not only the EAS

[15] *See, e.g.*, Saheed Oladimeji and Sean Michael Kerner, *SolarWinds Hack Explained: Everything You Need to Know*, TechTarget, June 29, 2022, found at https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (last visited December 19, 2022).

[16] *Id.*

equipment, but "all aspects of an EAS Participant's communications systems and services that potentially could affect their provision of EAS."[17] Since a station has to be operational and on the air to provide an EAS alert, this requirement potentially reaches nearly all station systems, not just those directly connected to the station's EAS equipment.

As proposed, the plan must contain a narrative discussion of "how the EAS Participant identifies 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."[18] But, the FCC will not read the plans,[19] will not provide training on how to create plans that will satisfy the FCC, and asks whether there are industry groups that can do that for them.[20] The FCC proposes that broadcasters can demonstrate they have complied with the threat assessment aspect of cybersecurity planning by following the NIST Risk Management Framework or the NIST Cybersecurity Framework.[21] In addition to this threat awareness section, the *NPRM* says that the cybersecurity plan must also "include security controls sufficient to ensure the confidentiality, integrity, and availability (CIA) of the EAS."[22] To meet this obligation, the *NPRM* says that EAS Participants can implement the Center for Internet Security's Critical Security Controls or CISA Cybersecurity Baseline. At a minimum, this portion of the plan would have to address issues like passwords, firewalls, software updates, multifactor authentication and wiping/disposal of old equipment.[23]

[17] *NPRM* at ¶ 27.
[18] *NPRM* at ¶ 23 (footnotes omitted).
[19] *NPRM* at ¶ 29.
[20] *NPRM* at ¶ 28.
[21] *NPRM* at ¶ 24.
[22] *NPRM* at ¶ 25.
[23] *NPRM* at ¶ 25.

All told, the *NPRM* estimates that it would take EAS Participants an average of just 10 hours per year to write, implement and continually update the cybersecurity plan.[24] The State Associations believe that the FCC severely underestimates the time involved in drafting, implementing, and monitoring a cybersecurity plan of the type the *NPRM* outlines, especially considering the harsh enforcement stance the *NPRM* takes and emphasis it places on non-stop threat assessment. The State Associations note that merely running the weekly and monthly tests and completing the log entries related to them at half an hour per week already amounts to 26 hours per year spent on the most baseline of EAS activities.

Designing a program to satisfy the multiple NIST frameworks and cybersecurity controls identified above involves hours of reading and researching those frameworks and controls before even beginning,[25] let alone the time involved in applying that learning, implementing the plan, and then continually monitoring the threat landscape.[26] Moreover, investigating even what initially *appears* could be an intrusion could take many hours by itself, and that is with regard to only a single occurrence. Even that assumes broadcasters have excess resources that are up to the task. It is likely that many small broadcasters do not have personnel on staff with sufficient extra hours available to undertake these initial and ongoing tasks and who have the training to do so. Accordingly, many would need to hire staff or third parties to assist them, at considerable cost.

[24] *NPRM* at ¶ 32.

[25] *See, e.g.*, Samuel Siskind, *Is NIST Compliance Worth It for SMBs? Costs vs Benefits*, networkassured.com, October 2, 2022, found at https://networkassured.com/security/nist-compliance/ (last visited December 22, 2022) ("Doing it yourself, while probably much cheaper, will ultimately require a lot of time and effort to just orient your staff to the various tasks.")

[26] *Id*. ("You should not have any illusions about going into NIST compliance. It is a major undertaking. The process can easily take six months and more in some cases . . . .").

The reward broadcasters can expect for undertaking all of this cybersecurity planning and effort is still strict liability and potential license renewal problems for any cybersecurity *or* EAS issue that might arise. According to the *NPRM*, having and even complying with a cybersecurity risk management plan does not provide any "safe harbor or excuse or any other diminishment of responsibility for negligent security practices."[27] Instead, the *NPRM* says:

> EAS Participants must remain constantly vigilant in preventing intrusions and can only satisfy that responsibility by acting reasonably in all circumstances. Any negligence in protecting the confidentially, integrity, and availability of EAS that results in transmission of false alerts or non-transmission of valid EAS messages would establish a violation of that duty, regardless of the content of the plan. Furthermore, we propose that an EAS Participant's failure to sufficiently develop or implement their plan, would be treated as a violation of the proposed rules.[28]

This enforcement stance threatens to undermine the partnership that has permitted the EAS to save thousands upon thousands of lives over the years in weather and other events despite being built largely on the backs of volunteers receiving no federal funding for organization or implementation. Faced with the possibility of enforcement actions and license renewal difficulties, broadcasters may seek to limit their involvement in the EAS wherever possible to avoid coming to the Commission's attention. PEP stations may no longer wish to serve in that role, placing entire states' EAS systems in jeopardy, and broadcasters and other EAS Participants may push back against continuing to carry non-Presidential Alerts with the added liability they would bring in the Commission's vision of the system.

Alternatively, the *NPRM* asks whether the FCC should simply identify a list of steps EAS Participants must take to secure their EAS equipment.[29] The FCC seems to fret that this

[27] *NPRM* at ¶ 30.

[28] *NPRM* at ¶ 30.

[29] *NPRM* at ¶ 26.

approach would lead to EAS Participants doing no more than what is on the checklist.[30] Yet, without more guidance as to what the FCC wants in cybersecurity plans, it seems likely that many EAS Participants will miss the mark, given the cost, time and technical sophistication required to draft, implement and maintain the plans. It also seems an unnecessary burden to impose when the FCC has not undertaken other productive approaches that would likely yield far more uniform and better results across the EAS ecosystem.

IV. Productive Alternatives to the FCC's Proposals Exist That Should be Explored and Funded First

The approach taken in the *NPRM* is one that places all of the burdens on the backs of EAS Participants like broadcasters to navigate complex issues of cybersecurity risk assessment and mitigation alone, when there are numerous roles the FCC could take on and avenues for public-private cooperation that could be pursued instead. Pursuing these foundational changes first will generate a better result for all, particularly the public, than focusing exclusively on the last link in the EAS distribution chain.

A. The FCC Should Work With EAS Equipment Manufacturers to Fund and Implement Uniform Solutions Across the EAS Ecosystem

A number of the solutions the FCC seeks could be implemented at the point of origin, through the EAS equipment itself, if the FCC were to work with manufacturers to implement those solutions and help fund these advances. For instance, the State Associations believe that EAS equipment manufacturers may already have the ability to directly notify users that have not updated their software of the need to do so. Similarly, EAS software could require users to reset passwords at regular intervals and even incorporate two-factor authentication. Finally, the EAS

[30] *NPRM* at ¶ 26.

equipment could incorporate its own dedicated firewall. Implemented at the source, these upgrades would uniformly increase security across the EAS ecosystem while needing to rely less on the vigilance of thousands of entry points into the EAS system.

But to build a more robustly secure (and therefore ever-evolving) EAS system, these requirements cannot simply be foisted on EAS equipment manufacturers or EAS Participants (through the costs of equipment upgrades and replacements). They must be funded. Having made the one-time sale of the EAS box itself, equipment manufacturers may not be able to offer continual software updates without charging for them. These charges can then price small EAS Participants out of compliance. The FCC should therefore make it a priority to secure funding for manufacturers to implement required upgrades, or to reimburse EAS Participants to ensure all are subscribed to receive ongoing upgrades, or both.

B. The Federal Government Should Fund and Encourage Use of More Secure Solutions than the Public Internet

Many of the FCC's concerns regarding the security of the interconnected EAS appear to stem from its reliance on the public Internet. The State Associations note that more secure alternatives exist and their use by Alert Originators and EAS Participants should be encouraged and funded. Working with both EAS equipment manufacturers and EAS Participants to identify and implement the most plausible alternatives (or develop new alternatives) would allow EAS systems to become largely isolated from the many points of vulnerability inherent in using the Internet as the backbone of the alert relay system.

C. The Commission Should Provide More Outreach, Guidance and Training to EAS Participants

The FCC should be seen as a source of ongoing and trusted information regarding cybersecurity for EAS Participants; one that helps them not only protect their EAS infrastructure, but their overall enterprise operations. Instead, the FCC sporadically sends emails about vulnerabilities in EAS equipment, but otherwise does not regularly engage with EAS Participants. Continuing engagement would promote discussions leading to innovations and solutions to issues like those that the *NPRM* seeks to address, as well as those arising in the future. For example, in the *NPRM*, the FCC predicates the need for a cybersecurity plan on the fact that in the August 2021 nationwide test, approximately 5,000 EAS Participants reported using out of date software or EAS equipment that was not capable of being updated.[31] Yet, to the State Associations' knowledge, the FCC has never followed up with any broadcasters or SECC Chairs to learn why it received those results. One EAS equipment manufacturer released multiple updates in close proximity to the time of the test. Perhaps some of the reporting was simple confusion as to which version was the most recent or in selecting the correct version from among multiple similar sounding versions available on the filing form. In other words, continuing engagement might determine better practices for determining whether EAS Participants are actually using out of date software, software that may not be the latest version but is still considered secure by the equipment manufacturer, or were merely confused by the FCC's system for reporting the EAS software version being used.

[31] *NPRM* at ¶ 22.

D. The FCC Should Reestablish the National Advisory Committee

Consistent with the above, the FCC should reinstate the National Advisory Committee or a similar EAS public-private forum for the exchange of information. As noted before, with more information from the FCC and FEMA regarding the outcome of the various Nationwide Periodic Tests, the SECC Chairs could reach out to EAS Participants in need of particular assistance to help them correct the issues they encountered in the test so that they do not recur. Similarly, the forum could help educate Alert Originators with regard to their cybersecurity responsibilities and need to secure password information, utilize multi-factor authentication, and install firewalls. As the EAS has expanded, many new and smaller Alert Originators are participating and able to send messages into the system. EAS Participants are thus ever more vulnerable to carrying an errant EAS message that has nothing to do with a failure in their own cybersecurity. An ongoing forum for the exchange of this type of information would help inform all parties and keep cybersecurity issues front of mind in a fast-changing world. Finally, the ongoing exchange of information could be extremely helpful in shaping the FCC's policy-making process.

V. If the FCC Adopts Any New Reporting Requirements, They Should Not Impose Unnecessary Burdens or Risks on Broadcasters

Should any FCC notification process be adopted in this proceeding, it should not impose unnecessary new burdens on broadcasters. For example, broadcasters should not be expected to learn to operate yet another new filing system like NORS that they do not already regularly use, particularly where a simple email might be far more efficient. Similarly, the State Associations agree with the *NPRM* that such filings should be kept confidential for a variety of reasons, not the least of which is to prevent these filings from becoming a resource for hackers, both with regard to who is vulnerable and to what types of attacks.

VI. The Proposed Implementation Timelines Are Too Short and Will Only Cause Confusion as to Proposed Compliance Dates

Finally, as the State Associations have pointed out in these Joint Comments, there are a number of productive steps the FCC should be taking before implementing any new reporting and cybersecurity risk plan requirements. If the FCC takes those steps, it will likely change the timelines proposed in the *NPRM* for when compliance with the various proposals would be required, if they are even retained. Regardless, the timelines proposed are far too short and invite confusion. For example, it is proposed that EAS Participants will not have to certify that they have implemented the proposed cybersecurity plan until the next Form One is filed. However, reporting of unauthorized access to station systems begins much sooner. Since much of the cybersecurity plan is directed at preventing the type of unauthorized access covered by the reporting requirement, EAS Participants could well become confused as to when the cybersecurity plan must be implemented and whether what they do to comply with the reporting requirement will be sufficient to allow them to certify compliance with the cybersecurity plan requirement at a much later date on the Form One. Accordingly, if any new requirements such as those proposed in the *NPRM* are ultimately adopted, a longer implementation timeline will be required, and the compliance timeframes sequenced to avoid creating such confusion.

CONCLUSION

For the reasons stated above, the State Associations respectfully request that the Commission retain the current rule allowing an automatic 60-day period for EAS equipment repair without specific Commission authority, avoid unnecessary reporting requirements and cumbersome reporting methods, assist EAS Participants with funding and training for any proposed upgrades to EAS software, hardware or cybersecurity, and revise its proposals in the *NPRM* consistent with these Joint Comments.

Respectfully submitted,

THE STATE BROADCASTERS ASSOCIATIONS

/s/ *Scott R. Flick*
Scott R. Flick
Lauren Lynch Flick

Pillsbury Winthrop Shaw Pittman LLP
1200 Seventeenth Street, NW
Washington, DC 20036
(202) 663-8000

December 23, 2022