

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

In the Matter of

Modernization of the Nation's Alerting Systems	)	PS Docket No. 25-224
	)	
Protecting the Nation's Communications Systems	)	PS Docket No. 22-329
from Cybersecurity Threats	)	
	)	
Wireless Emergency Alerts	)	PS Docket No. 15-91
	)	
Amendment of Part 11 of the Commission's Rules	)	PS Docket No. 15-94
Regarding the Emergency Alert System	)	

**COMMENTS OF THE
NATIONAL ASSOCIATION OF BROADCASTERS**

1 M Street, SE
Washington, DC 20003

Rick Kaplan
Larry Walke
Kelly Williams
David Layer

August 29, 2026

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY	1
II.	THE FCC IDENTIFIES THE SALIENT ISSUES REGARDING A SOFTWARE-BASED EAS MODEL AND SETS A REASONABLE COURSE TOWARD VOLUNTARY ADOPTION	3
A.	NAB Supports a Flexible, Local Approach to EAS Software	5
B.	A Software-Based EAS Model Could Help Alleviate Supply Chain Concerns	6
C.	NAB Supports the Testing and Certification of EAS Software	8
D.	Requiring Tested, Trusted EAS Software to Run on Trusted Hardware Should Minimize Cybersecurity Risks.....	12
E.	The FCC Should Wait to Modify the Deadline to Repair or Replace Defective EAS Software Until it Can Establish a Policy Based on Real-World Experience	14
III.	NAB GENERALLY SUPPORTS THE OTHER PROPOSALS IN THE FURTHER NOTICE DESIGNED TO ENHANCE EAS.....	16
A.	Securing EAS Through Message Authentication.....	16
B.	Preventing Duplicate Alerts Through a Universal Identifier	18
C.	Improving the Accuracy of Alert Geotargeting.....	19
IV.	PROMOTING THE USE OF SYMBOLS FOR ALERTS.....	21
V.	CONCLUSION	24

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

In the Matter of

Modernization of the Nation's Alerting Systems	)	PS Docket No. 25-224
	)	
Protecting the Nation's Communications Systems	)	PS Docket No. 22-329
from Cybersecurity Threats	)	
	)	
Wireless Emergency Alerts	)	PS Docket No. 15-91
	)	
Amendment of Part 11 of the Commission's Rules	)	PS Docket No. 15-94
Regarding the Emergency Alert System	)	

**COMMENTS OF
THE NATIONAL ASSOCIATION OF BROADCASTERS**

I. INTRODUCTION AND SUMMARY

The National Association of Broadcasters (NAB)¹ hereby submits comments on the above-captioned Further Notice of Proposed Rulemaking, in which the Commission proposes certain policy and technical updates intended to improve the effectiveness and security of the Emergency Alert System (EAS).² Given the unique role that America's local television and

¹ The National Association of Broadcasters (NAB) is a nonprofit trade association that advocates on behalf of free local radio and television stations and broadcast networks before Congress, the Federal Communications Commission (Commission or FCC), and other federal agencies, and the courts.

² *Modernization of the National Alerting Systems*, PS Docket No. 25-224, *Protecting the Nation's Communications Systems from Cybersecurity Threats*, PS Docket No. 22-329, *Wireless Emergency Alerts*, PS Docket No. 15-91, *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System*, PS Docket No. 15-94, Report and Order in PS Docket Nos. 25-224 and 22-329 and Further Notice of Proposed Rulemaking in PS Docket Nos. 25-224, 15-94, and 15-91 (rel. June 29, 2026) (Order or Further Notice). The Order and Further Notice also address certain changes to Wireless Emergency Alerts (WEA) not discussed herein.

radio stations serve as the “backbone” of EAS,³ we strongly support the FCC’s ongoing efforts to improve the system.

In particular, we applaud the Commission’s grant of NAB’s Petition for Rulemaking to consider rules changes that would allow EAS Participants to voluntarily use a software-based model for processing EAS messages instead of a physical hardware device as required under the current rules.⁴ NAB believes that aligning EAS with modern broadcasting systems operate is critical to its future efficiency and reliability, and thus welcomes the FCC’s thorough analysis of our Petition in the Further Notice. Below, we support the FCC’s findings regarding the public safety benefits of a software-based EAS option and seek to helpfully address the insightful questions raised in the Further Notice.⁵ For example, we agree with the FCC that requiring EAS software to be tested and certified through a process similar to that used for existing EAS equipment would be appropriate.⁶ We are optimistic that some of the Telecommunications Certification Bodies (TCBs) already approved by the FCC to certify EAS devices can perform conformity testing of EAS software, or would develop this capability in response to market demand if a software approach is permitted. NAB also supports the Commission’s focus on the cybersecurity of EAS software, and agrees that providers of EAS software should be responsible for demonstrating the cybersecurity of their software.⁷ On the other hand, we believe it is premature to reduce the required time for repairing or

³ *AM Radio: Backbone of the Emergency Alert System*, WMAL (Aug. 5, 2025) (quoting Troy A. Miller, President & CEO, National Religious Broadcasters Association), <https://www.wmal.com/2025/08/05/am-radio-backbone-of-the-emergency-alert-system/>.

⁴ Petition of the National Association of Broadcasters for Emergency Alert System Modernization, PS Docket Nos. 15-94 and 22-329 (filed Mar. 31, 2025) (NAB Petition).

⁵ Further Notice at ¶¶ 94-95.

⁶ Further Notice at ¶ 106.

⁷ *Id.* at ¶¶ 111-112.

replacing defective EAS software from 60 days to 72 hours.⁸ There are still too many uncertainties around the implementation of EAS software to change the deadline at this time. Instead, NAB respectfully asks the FCC to retain the existing 60-day deadline for EAS software and revisit this issue in the future when it can establish a new policy with the benefit of real-world experience.

Regarding other issues in the Further Notice, NAB generally has no objections to the FCC's proposals for improving the authentication or geotargeting of EAS alerts, using a universal alert identification number to reduce duplicative alerts, or integrating visual symbols into EAS.⁹ However, we respectfully caution the Commission against imposing additional mandates that could outstrip the capabilities of existing EAS devices and require broadcasters to purchase new EAS equipment. We also ask the FCC to avoid reducing the automated simplicity of EAS or limiting broadcasters' ability to provide EAS alerts consistent with their journalistic judgement.

II. THE FCC IDENTIFIES THE SALIENT ISSUES REGARDING A SOFTWARE-BASED EAS MODEL AND SETS A REASONABLE COURSE TOWARD VOLUNTARY ADOPTION

The FCC correctly frames the proposed software-based EAS model as an opportunity to better integrate EAS into modern broadcasting IP-centric air chains, enhance public safety, and reduce unnecessary regulatory burdens on EAS Participants.¹⁰ Like other modern broadcast operations, a software approach would facilitate remote EAS operations, monitoring, and collection of performance data. This approach will also promote resiliency by enabling EAS operations to be located at multiple local or edge locations and will optimize

⁸ *Id.* at ¶ 114.

⁹ *Id.* at ¶¶ 41-56, 70-75, and 78-82.

¹⁰ *Id.* at ¶¶ 88-89.

maintenance by preventing the need to physically diagnose and repair problems within an EAS hardware device.¹¹ Importantly, use of EAS software would be optional; nothing in the FCC’s proposal would affect EAS Participants who prefer to continue on a hardware path. NAB highlighted other benefits of this approach in our Petition, including the swift application of upgrades through software patches in response to security updates or FCC rules changes and improved EAS message routing to separate broadcast streams.¹²

The FCC asks whether a software-based EAS model would allow EAS Participants to better “analyze, process, and present audio/visual messages, photos, maps, or other information provided or linked in a CAP EAS alert . . . or [perform] geotargeting calculations, text-to-speech, speech-to-text, or other alerting functions?”¹³ NAB submits that a software-based model could facilitate all of these functions. Currently, EAS functionality is housed within proprietary hardware devices that often require stations to schedule an engineer to physically visit all their EAS boxes to add new capabilities. On the other hand, if EAS software is permitted to reside on a server or elsewhere in a station’s secure air chain, adding such functions could be accomplished by remotely implementing a simple software upgrade.

Moreover, there may be a significant number of existing EAS devices for which adding certain functionalities to comply with new FCC regulations could require the device to be returned to the manufacturer for hardware modification or the purchase of a new device,

¹¹ *Id.* at ¶ 90 citing Comments of CMG Media Corporation, PS Docket Nos. 15-94 and 22-329 (May 2, 2025), at 2; Comments of the Society of Broadcast Engineers, Inc., PS Docket Nos. 15-94 and 22-329 (May 2, 2025), at 4; Comments of NCTA – The Internet & Television Association, PS Docket Nos. 15-94 and 22-329 (May 2, 2025), at 6-10.

¹² NAB Petition at 6-7.

¹³ Further Notice at ¶ 95.

thus hindering widespread, equitable adoption.¹⁴ Software has far fewer limitations and would be more likely to efficiently accommodate additional capabilities.

A. NAB Supports a Flexible, Local Approach to EAS Software

NAB agrees with the Commission that flexibility should be the watchword of a software-based EAS model, and thus supports the FCC's proposal to allow EAS Participants to install EAS software in a single server or computer that manages a station's EAS functions, or within multiple components to facilitate cross-system integration.¹⁵ This approach should help stations economize integration of EAS software into a station's air chain (i.e., server), or into a vendor's transmitter/signal processing systems.¹⁶ In addition, looking ahead, allowing a software model could potentially facilitate integration of EAS operations into an efficient consolidated suite of software systems that, for example, runs a station's weather information, advertising traffic, ratings data, and other functions. Permitting stations to optimize their air chain by customizing integration of EAS software should help "improve EAS continuity, security, flexibility, and agility."¹⁷

Moreover, a software approach will promote resilient, redundant EAS operations that can be located at both a station's studio or transmitter, allowing immediate fail-over if the

¹⁴ For example, the FCC required broadcasters to purchase new equipment when it replaced the Emergency Broadcast System with EAS. *Amendment of Part 73, Subpart G, of the Commission's Rules Regarding the Emergency Broadcast System*, Report and Order and Further Notice of Proposed Rulemaking, 10 FCC Rcd 1786, 1828 (1994). More recently, the FCC conceded that compliance with rules it proposed following the first nationwide EAS test in 2013 could require broadcasters to replace EAS hardware. *Review of the Emergency Alert System*, Notice of Proposed Rulemaking, 20 FCC Rcd 8123, 8143 (2014).

¹⁵ Further Notice at ¶ 96.

¹⁶ *Id.*

¹⁷ Comments of Aldon Caron, KPOV-FM, PS Docket Nos. 15-94 and 22-329 (April 28, 2025); Joint Comments of New York Public Radio, University Radio Foundation, Inc., and J. Paxton Durham, Chairman, Roanoke, VA Extended EAS Operational Area, PS Docket Nos. 15-94 and 22-329 (May 2, 2025), at 4.

software's primary location is inaccessible due to fire, flood, or other disaster.¹⁸ That said, NAB again emphasizes that we do not support a fully cloud-based system for processing EAS messages,¹⁹ given the increased risks of a security breach or a power outage that could cut stations off from their EAS operations at the most inopportune time.

It is for this reason that local broadcasters are crucial to EAS. The uniquely reliable architecture of broadcasting allows local stations to keep the public informed and safe during emergencies, even when power outages render cable news programming useless and telecommunications platforms fail. Cell sites were offline for four days during the 2023 wildfires in Maui, Hawaii,²⁰ almost two weeks in parts of North Carolina during Hurricane Helene in 2024,²¹ and for up to three weeks in some parishes in Louisiana during Hurricane Ida in 2021.²² And yet, local broadcasters remained on-the-air to deliver EAS warnings and emergency information during all these disasters, and have no interest in undermining their matchless emergency public service through a fully cloud-based broadcast EAS system.

B. A Software-Based EAS Model Could Help Alleviate Supply Chain Concerns

The Commission seeks comment on market-based justifications for allowing the use of software EAS, such as whether this approach may reduce supply chain concerns or encourage more vendors to enter the EAS market.²³ Digital Alert Systems, Inc. (DAS) argues

¹⁸ NAB would not object to allowing local broadcast stations to locate EAS software at locations other than the studio or transmitter as a backup in case of a catastrophe that damages both the studio and transmitter.

¹⁹ NAB Petition at 4.

²⁰ See, e.g., FCC, *Communications Status Report for Areas Impacted by Hawaii Wildfires* (Aug. 19, 2023), <https://docs.fcc.gov/public/attachments/DOC-396155A1.pdf>.

²¹ Congressional Research Service, *Restoration of Cell Phone Services: Hurricane Helene* (Oct. 8, 2024), <https://www.congress.gov/crs-product/IF12779>.

²² See, e.g., FCC, *Communications Status Report for Areas Impacted by Hurricane Ida* (Sep. 9, 2021), <https://docs.fcc.gov/public/attachments/DOC-375605A1.pdf>.

²³ Further Notice at ¶¶ 100-102.

that supply chain concerns should not be assigned to all EAS manufacturers. DAS also claims that allowing a software EAS approach could reduce demand for hardware devices and lead to less investment and innovation in EAS hardware performance.²⁴

NAB submits that a software approach could ease overall supply chain problems because software does not have to rely on the manufacture of the purpose-built, physical hardware components for new or replacement proprietary EAS boxes in which software is housed. Nor would EAS equipment have to be shipped to manufacturers or EAS Participants. Software can also reduce the need for station staff to manually repair EAS boxes, or ship boxes to manufacturers for repair.²⁵ We have already seen an example of the problems that can be caused by reliance on hardware. Due to delays in the delivery of a needed firmware update by an EAS equipment manufacturer, many stations were unable to meet a deadline in December 2023 to comply with a new FCC requirement to prioritize the transmission of CAP-formatted EAS alerts. The singular deadline also caused many EAS Participants to request the help of engineering consultants at the same time, including many station groups with “dozens or even hundreds of EAS boxes” that were located at remote locations.²⁶ The Commission conceded that compliance would be impracticable for many EAS Participants and delayed compliance by 90 days. A software approach would help avoid such issues.

The Commission has determined in other contexts that software can help reduce supply chain concerns. For example, in March 2021, with then-Commissioner Carr’s concurrence, the FCC sought comment on Open Radio Access Networks (Open RAN) as a

²⁴ *Id.* at ¶ 101 citing Comments of Digital Alert Systems, Inc (DAS), PS Docket Nos. 15-94 and 22-329 (May 2, 2025), at 29.

²⁵ Further Notice at ¶ 114.

²⁶ *Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System*, Order, 38 FCC Rcd 11034 (Nov. 28, 2023).

potential path to drive 5G innovation.²⁷ The FCC stated: “Open and virtualized radio access networks have the potential to address . . . concerns that the Commission and other federal stakeholders have raised in recent years about . . . supply chain reliability.”²⁸ The FCC noted other potential benefits of an Open RAN approach, including the diversification of technical solutions and vendors, more efficient network security monitoring, and enhanced innovation and interoperability.²⁹ The parallels to a software-based EAS approach are clear.

Regarding DAS’s other claims, broadcasters appreciate DAS’s inventory management and understand that supply chain concerns may not apply equally to all EAS manufacturers. However, thousands of EAS Participants use hardware EAS devices from other manufacturers and will continue to do so for many years, if not forever, even if a software option is allowed. We believe that EAS manufacturers will not abandon their hardware customers in the interim.

Finally, we disagree with the premise of DAS’s claim that allowing a software approach will reduce investment in EAS hardware. The potential stifling of innovation in EAS hardware is no reason to stifle the innovation of EAS software. Under this view, personal computers may have been delayed to protect word processors, and mobile phones delayed to preserve landlines and payphones.

C. NAB Supports the Testing and Certification of EAS Software

NAB agrees with the FCC that EAS software should be tested and approved under a conformity assessment system before it can be marketed and used,³⁰ and that the process

²⁷ *Promoting the Deployment of 5G Open Radio Access Networks*, Notice of Inquiry, 36 FCC Rcd 5947 (2021).

²⁸ *Id.* at 5949.

²⁹ *Id.* at 5949-5950.

³⁰ Further Notice at ¶ 104.

should be similar to that used for existing EAS equipment.³¹ We see no reason that part 2 of the rules cannot be applied to EAS software, with a few minor changes.

Like the current process, a software developer or entity seeking to market and sell EAS software should be responsible for running its product through the testing and certification process, including arranging for the software to be tested by an accredited FCC-recognized test laboratory, and submitting the certification application to a telecommunication certification body (TCB) for review. The Commission states that such test labs are typically focused on measuring RF emissions from hardware devices, power levels, and other frequency-related outputs, and asks if they are equipped to test EAS software.³²

NAB would defer to the expertise of EAS manufacturers on these questions, but if needed, we would be willing to enlist broadcasters to help determine the features and functions of EAS software that should be tested. That said, we understand that EAS manufacturers have routinely tested the functionality of EAS equipment for the past 15 years; therefore, the most efficient approach may be to allow EAS manufacturers to continue this practice for EAS software. Alternatively, we believe that some TCBs may be able to test the EAS functionality of EAS hardware devices and could possibly do the same for EAS software allowed under the FCC's proposal, or if not, would develop this capability in response to market demand created by an approved EAS software option.

NAB believes that the part 2 rules appear broad enough to cover the advent of EAS software. For example, Section 2.915 states that a TCB will “grant an application for certification if it finds from an examination of the application and supporting data . . . that:

(1) The equipment is capable of complying with pertinent technical standards of the rule

³¹ *Id.* at ¶ 106.

³² *Id.*

part(s) under which it is to be operated as well as other applicable requirements.”³³ This seems to indicate that EAS software capable of complying with the technical standards for EAS, as set forth in Part 11 of the FCC’s rules, would be eligible for certification.

NAB agrees with the FCC that Part 11 could be applied to EAS software through some minor updates,³⁴ and supports the FCC’s approach in Appendix B of the Further Notice, including a proposed new definition of “EAS Software,” and changes to the rules governing EAS encoders and decoders, equipment acceptability, and certain other sections.³⁵ Also, the FCC can always amend the rules further to resolve any issues that arise during the roll-out of EAS software.

The Commission also asks whether certain modifications to EAS software should require recertification.³⁶ Under the FCC’s rules, certain kinds of changes to FCC-authorized equipment are classified as permissive changes that must be recertified. For example, a Class I permissive change includes changes to equipment that “do not degrade the characteristics reported by the manufacturer and accepted by the Commission when certification is granted.” Such changes require no filing with the FCC.³⁷ Class II permissive changes include changes which degrade the performance characteristics reported to the FCC when equipment was first certified but still meet the minimum requirements of the rules. Entities responsible for such changes must submit certain information to the FCC, including the results of tests of the performance characteristics affected by the change.³⁸

³³ 47 C.F.R. § 2.915.

³⁴ Further Notice at ¶ 108.

³⁵ *Id.* at Appendix B.

³⁶ *Id.* at ¶ 110.

³⁷ 47 C.F.R. § 2.1043(b)(1).

³⁸ *Id.* at § 2.1043(b)(2).

NAB submits that future changes to EAS software that do not degrade performance should be treated as a Class I permissive change, including changes in response to FCC rules changes and upgrades to address functional or security issues. First, we note again that current EAS encoding and decoding is driven by software that is housed within a proprietary hardware device. Over the years, EAS manufacturers have made numerous updates to their equipment's functionality,³⁹ due to technical innovations as well as FCC rules changes.⁴⁰ To our knowledge, none of these updates required recertification by the FCC, and we see no reason why similar changes to EAS software that happens to not be housed within a hardware device should be treated differently. Second, requiring recertification of such changes could delay implementation of software upgrades, including updates to resolve security vulnerabilities.

For the same reasons, periodic recertification of EAS software is unnecessary. The FCC is concerned that EAS software may be used after it is no longer supported by a vendor,⁴¹ but again, this would be no different than EAS boxes that are no longer supported by a vendor. Instead of periodic recertification, NAB submits that a case-by-case determination of whether recertification is needed would be more appropriate, given the range of circumstances that could lead to an issue.

³⁹ See, e.g., Digital Alert Systems Updates EAS Software, Radio World (Nov. 20, 2024), <https://www.radioworld.com/tech-and-gear/products/digital-alert-systems-updates-eas-software>.

⁴⁰ See, e.g., Digital Alert Systems Releases DASDEC V5.2, Radio World (Oct. 17, 2023), https://www.radioworld.com/tech-and-gear/products/digital-alert-systems-releases-dasdec-v5-2?utm_term=594DDF2B-73C1-4BD4-8F3C-F1056190969A.

⁴¹ Further Notice at ¶ 110.

D. Requiring Tested, Trusted EAS Software to Run on Trusted Hardware Should Minimize Cybersecurity Risks

NAB supports the FCC's focus on the cybersecurity of EAS software. As previously explained, a software approach will improve EAS security by facilitating updates to address security vulnerabilities through a simple software patch instead of forcing station personnel to manually upgrade all of their EAS boxes or ship the boxes to a manufacturer.⁴² This will greatly reduce EAS downtimes while security problems are fixed.

We also stress again that we do not support a cloud-based model. Instead, we envision autonomous software-based EAS functions located on premises at the edge of a broadcaster's operation, like other secure software systems used in modern broadcast systems. This model would not be directly exposed to the internet and would still operate if internet connectivity is disrupted. The software-based EAS functions of decoding, logging, encoding, and relaying alerts will act autonomously, as in legacy EAS hardware devices. Under this approach, EAS functionality would be no more vulnerable to unwanted IP-based attacks or disruptions than existing hardware EAS boxes.⁴³

A software-based approach should not raise any exceptional issues compared to existing hardware devices.⁴⁴ As Sage notes, a software EAS mode is not inherently different than existing EAS hardware, and not fundamentally different than other parts of a modern broadcast air chain.⁴⁵ Many types of broadcast equipment have IP-network connections that enable remote access for system monitoring, software updates, and receipt of metadata

⁴² NAB Petition at 6.

⁴³ *Id.* at 4.

⁴⁴ Letter from Harold Price, President, Sage Alerting Systems, Inc., to Ms. Marlene Dortch, Secretary, FCC, PS Docket Nos. 15-94 and 22-329 (June 9, 2025) (June 2025 Sage Letter).

⁴⁵ Letter from Harold Price, President, Sage Alerting Systems, Inc., to Ms. Marlene Dortch, Secretary, FCC, PS Docket Nos. 15-94 and 25-224 (May 14, 2026), attachment at 18.

programming, all of which also need to prevent unauthorized access to a station's air chain. Broadcasters are already familiar with operating critical systems using enterprise cybersecurity controls, such as authentication, management of update patches, network segmentation, and risk mitigation practices, and would do the same for EAS software.

EAS software, like existing hardware devices, would be just one part of a broadcaster's system, and every part is important in preventing unauthorized disruptions. Treating software EAS differently, such as mandating extraordinary monitoring or periodic recertification, without mandating similar requirements for all other parts of the air chain, would increase the costs to provide EAS without meaningfully improving the overall security of a broadcaster's facility.⁴⁶

Thus, we support Sage's approach that calls for EAS software from only a "trusted source running on curated hardware, meaning hardware provided by the trusted source, or curated software running in a curated environment within another product such as a transmitter, processor, audio router, playout system, etc., where that hardware is from a trusted source."⁴⁷ We believe that cybersecurity risks would be minimized so long as EAS software is certified and operating in a documented, supported, and secure environment, which could include vendor-provided hardware (as is the current practice), secure servers controlled by an EAS Participant, or integration within other broadcast equipment, and provided implementation meets the Part 11 rules and applicable cybersecurity controls.

As under current practice, the FCC should rely on EAS software providers to follow reasonable cybersecurity best practices and self-certify the security of their product.⁴⁸ Radio

⁴⁶ *Id.*, attachment at 20.

⁴⁷ *Id.*, attachment at 19.

⁴⁸ DAS's claims that allowing the use of a software-based EAS model will somehow shift many responsibilities for securing EAS from manufacturers to EAS Participants should be

and television stations take their commitment to EAS seriously, and will not risk harming their reputation, or FCC enforcement. Accordingly, NAB believes that EAS Participants will insist on nothing less than an EAS vendor's best efforts to ensure the effectiveness and security of their product from any EAS system they choose. This approach, together with the new cybersecurity measures adopted in the Order,⁴⁹ should alleviate any cyber concerns uniquely related to EAS software.

E. The FCC Should Wait to Modify the Deadline to Repair or Replace Defective EAS Software Until it Can Establish a Policy Based on Real-World Experience

The Commission proposes to reduce the deadline for EAS Participants to repair or replace defective EAS equipment from 60 days to 72 hours for EAS software models.⁵⁰ The FCC states that, although 60 days is usually sufficient for the repair defective hardware devices, the record suggests that a shorter amount of time would be reasonable for EAS software models because they should be reparable through a patch or other remote fix. The FCC further states that "EAS software may be more prone to cyberattack by virtue of its IP interconnectedness," creating a "heightened need for Commission awareness of lingering EAS software defects that may derive from ransomware, viruses, or other cyberattacks."⁵¹ Thus, the Commission finds that 72 hours is a reasonable amount of time for an EAS

dismissed. Further Notice at ¶ 113. These are nothing more than red herrings to dissuade the FCC against potentially opening the EAS marketplace to more competitors. Sage notes that DTS Autostage, Quu, RadioDNS, NPR ContentDepot and other systems all have similar needs to prevent unauthorized access to the air chain. May 2026 Sage Letter, attachment at 18. Of course, contrary to DAS's claims, none of these require local radio and TV stations to implement secure hardware configurations, maintain firmware integrity, perform vulnerability testing, or ensure end-to-end system hardening, as DAS claims the use of EAS software would require.

⁴⁹ Order at ¶¶ 18-27.

⁵⁰ Further Notice at ¶ 114 citing 47 CFR § 11.35(b).

⁵¹ *Id.* at ¶ 114.

Participant using EAS software to either implement repairs or switch over to backup software while repairs of the software in its main facility are completed.

As a preliminary matter, NAB respectfully disagrees with the notion that a software-based model would be more prone to cyber-related disruptions than hardware devices. Again, NAB only supports an approach that requires tested, trusted, and curated software code running on trusted hardware, and one not directly exposed to the internet any more than existing hardware devices.

Reducing the 60-day deadline to repair defective EAS software to 72 hours would be impractical because, pursuant to the Commission's rules, EAS Participants test the functionality of their EAS systems and review the logs of such tests weekly at most.⁵² Thus, barring an actual alert, it could be unlikely that an entity would discover a problem with their EAS software within 72 hours unless the problem happens to arise three or fewer days before a weekly test.

Moreover, in many cases, a problem with a software-based model could have nothing to do with the software itself, but instead related to the server, computer, or other hardware on which the software runs, or the firewall or some other component. Recovery could depend on validated images, reconfiguration, vendor support, and possibly replacement of hardware. Also, in many instances, it would likely take longer than 72 hours to pinpoint the root of the problem and effectuate a repair, especially if the problem is related to hardware that must be repaired or replaced.

Accordingly, NAB submits it is premature to reduce the 60-day timeframe to 72 hours. There are too many uncertainties surrounding the testing and certification of EAS

⁵² 47 C.F.R. § 11.61(b).

software, how widely this voluntary approach will be adopted, the types of EAS software that may be offered, how software will be implemented (e.g., alone or packaged with other broadcast software systems), and vendor support. Instead, we respectfully ask the Commission to retain the existing 60-day deadline for EAS software and revisit this question in the future when it can establish a policy with the benefit of real-world experience.

III. NAB GENERALLY SUPPORTS THE OTHER PROPOSALS IN THE FURTHER NOTICE DESIGNED TO ENHANCE EAS

As set forth below, NAB has no objections to the Commission's proposals regarding authentication and geotargeting of EAS alerts, a universal alert identification number, or visual symbols, provided any new mandates do not force broadcasters to buy new EAS equipment, reduce the automated simplicity of EAS, or affect broadcasters' editorial discretion to present EAS alerts.

A. Securing EAS Through Message Authentication

The Commission states that the use of digital signatures can help protect EAS from the unauthorized disruption or falsification of EAS alerts by securing handoffs between alert originators and EAS Participants that relay EAS messages to the public. Currently, CAP-formatted EAS alerts that are issued through IPAWS include digital signatures that require EAS Participants to reject EAS messages that include an invalid digital signature. However, the FCC's rules still allow EAS Participants to transmit EAS messages that lack any digital signature at all. The Commission proposes to close this gap by requiring EAS Participants to reject CAP EAS messages that do not include a valid digital signature.⁵³

⁵³ Further Notice at ¶¶ 41-42.

NAB agrees with the Commission that ensuring the security and reliability of EAS is critical to maintaining public confidence in the system,⁵⁴ and supports the FCC's approach. We would defer to the expertise of EAS manufacturers, although it appears that meeting this obligation would not be unduly burdensome because EAS equipment is already required to authenticate IPAWS originated CAP EAS messages that include a digital signature.⁵⁵ To facilitate adoption, however, the FCC should consider a phased approach to implementation. It would also be helpful if the FCC or the FEMA/IPAWS program office provides clear guidance on the issuance, rotation, and revocation of signatures⁵⁶ that is tailored to the resources and circumstances of broadcasters and other EAS Participants. For example, it would be efficient if signature failures generated actionable operator alerts and log entries, instead of mere silent rejections.

The Commission also seeks comment on the feasibility of requiring EAS Participants to authenticate legacy EAS messages, although the FCC recognizes that legacy EAS, which is transmitted using the legacy SAME-based EAS protocol, is limited in how much data it can carry. Adding data to authenticate legacy EAS messages could delay transmission of alerts to EAS Participants, and in turn, broadcast of EAS messages to the public.⁵⁷ Again, although we strongly support improving the security of EAS, we are wary of new rules that could

⁵⁴ *Id.* at ¶ 42. See also CSRIC VI, *Final Report—Security Aspects of Emergency Alerting System (EAS)* at 27, 33-34 (2018), <https://www.fcc.gov/file/14853/download> (CSRIC VI EAS Security Report).

⁵⁵ *Id.* at ¶ 42.

⁵⁶ *Cryptographic Key Management in 2025 and Beyond*, Cryptomathic (June 24, 2025), <https://www.cryptomathic.com/blog/cryptographic-key-management-in-2025>; Carla Mendoza, *Best Practices in Certificate Lifecycle Management*, GlobalSign by GMO (Oct. 9, 2023), <https://www.globalsign.com/en/blog/best-practices-in-certificate-lifecycle-management>.

⁵⁷ Further Notice at ¶¶ 45-47.

impede access to EAS or require additional data processing beyond the capacity of existing EAS devices. We also note that most EAS alerts are issued by the National Weather Service (NWS), which transmits weather-related alerts over NOAA Weather Radio in the legacy EAS protocol. Thus, until the NWS implements a mechanism for digitally signing or otherwise authenticating their alerts, the benefits of requiring EAS Participants to upgrade or replace equipment to process digitally signed legacy messages may be limited. Overall, NAB would support any FCC measures designed to improve the security of EAS alerts, provided implementation is simple, cost-effective, and broadly impactful.

B. Preventing Duplicate Alerts Through a Universal Identifier

The FCC states that public warning stakeholders expect alerts to be presented once and that duplicate alerts can cause public confusion and alert fatigue. To address these concerns, the FCC proposes to require Participating Commercial Mobile Services providers that deliver WEA messages to identify whether an alert is a duplicate through the use of a common message identifier, also known as a “universal alert message ID,” that would be assigned to every WEA message they receive.⁵⁸ The Commission also seeks comment on implementing a universal alert message ID in EAS, and if so, if it would help prevent duplicate EAS messages. For example, if an EAS device discerns any difference in the message header information of an EAS alert from a previously received message about the same event, it will not be deemed a duplicate and will relay a repetitive message.⁵⁹

NAB members report that duplicate alerts are not a major problem in the EAS ecosystem. In their experience, duplicate EAS alerts occur in only a couple of rare situations, neither of which would be resolved by a universal alert identification number. For example,

⁵⁸ *Id.* at ¶ 51.

⁵⁹ *Id.* at ¶ 55.

there is a small number of well-meaning broadcast stations, including LP stations, that sometimes edit alerts before broadcasting to tailor the messages to their local communities. In some cases, other stations that monitor those stations for alerts may automatically relay largely duplicate alerts about the same event that it receives from the LP station and also directly from IPAWS or the alert originator. Another circumstance can arise if an alert is issued for a mountainous area. Radio transmitters on the east and west side of a mountain will receive and relay only one EAS alert, but individuals located to the south or north of the mountain may receive duplicate alerts from both transmitters.

If the FCC decides to act in this area, NAB supports an approach that is driven by FEMA/IPAWS and does not create new station-side workflow or equipment complexity that outstrips the capabilities of existing EAS equipment. It is also important that any duplicate-suppression mechanism clearly distinguish between genuine duplicates and legitimate alert updates, corrections, cancellations, extensions, and other material changes, which is critical for weather and other fast-moving emergencies.

C. Improving the Accuracy of Alert Geotargeting

The FCC expresses support for improved geotargeting of emergency alerts because alerting people about situations that are not geographically relevant to them can dilute urgency and trust in alerts about emergencies that are relevant to them.⁶⁰ Some commenters also suggest that poor geotargeting of alerts can affect alert originators' inclination to use public warning systems.⁶¹ The FCC explains that EAS Participants are

⁶⁰ *Id.* at ¶ 60; Comments of Shawn Williams, PS Docket No. 25-224 (Aug. 11, 2025), at 1.

⁶¹ *Id.* citing Comments of New York City Emergency Management, PS Docket No. 25-224 (Sep. 9, 2025), at 5.

currently restricted to targeting alerts based on county codes,⁶² which limits their ability to geotarget alerts to smaller areas.⁶³ Many CAP- based emergency messages, including WEA, support more detailed circles or polygons that can target alerts to areas smaller than a county. The FCC seeks comment on whether EAS Participants would be interested in using certain additional data, such as circles and polygons, or partial county alert (PCA) code or additional fixed EAS location codes, in deciding which state and local alerts to broadcast.⁶⁴

While NAB does not oppose the use of PCA codes, it is unclear whether including PCA codes in EAS transmissions would fix the problem the FCC seeks to solve. NAB understands that the answer may depend on the distinction between CAP-formatted and legacy SAME-based EAS dissemination. In the former environment, circles and polygons may provide stations with more useful data when choosing whether to relay an alert, such as whether the station's signal covers the areas described by the circle or polygon. However, the Commission should be mindful of the inherent limitations in translating a circle or polygon contained in a CAP-based alert to a PCA code in a SAME-base EAS message, because the circles and polygons do not map cleanly to counties and sub-counties. The NWS has long struggled with this issue in trying to adapt CAP-based alerts for distribution via NOAA weather radio.

Also, legacy EAS is a broader public warning path⁶⁵ that is generally delivered through specific audio, text crawl, and display formats and could be ill-suited for a precise location-

⁶² 47 CFR § 11.31(e).

⁶³ Further Notice at ¶ 70.

⁶⁴ *Id.*

⁶⁵ The unique advantage of broadcasting is the ability to reach broad areas at the same time, and many broadcasters feel strongly that local television and radio service is already sufficiently geotargeted within their service contours. They also point out that the use of

aware, end-user targeting system. Broadcasters already experience some overlapping and unnecessary alerting caused by the interaction between polygon-based warnings issued by NWS and legacy EAS county-based alerting. Introducing additional geographic segments within each county risks creating even more alert noise without making legacy EAS truly location aware. The additional information may also make alerts harder to understand and dilute attention to the most essential elements of an alert.⁶⁶ Accordingly, NAB supports allowing EAS Participants to consider CAP polygons and circles where useful as optional data that can enhance alerting decisions, but not mandating or encouraging migration toward more complex fixed PCA-based geography descriptors in legacy EAS.

IV. PROMOTING THE USE OF SYMBOLS FOR ALERTS

The Commission seeks comment on whether to require EAS messages to display certain visual symbols that identify the type of emergency at hand.⁶⁷ NAB agrees that symbols could potentially improve the understanding of, and public response to, EAS alerts, and generally supports the FCC's proposal subject to certain conditions.

circles and polygons would not affect the area covered by a television or radio station's signal, which of course does not stop at county or state borders.

⁶⁶ The FCC's Monroe County, Florida/Key West example illustrates the limitation. *Id.* at ¶ 73. If a directional partial-county label such as "Southwest Monroe County" does not communicate "Key West" to the public, then the problem is not merely the lack of an additional partial county code. The challenge is that many neighborhoods, islands, corridors, valleys, and other locally understood areas in Monroe County do not map cleanly to the legacy EAS county-based plus partition approach. Attempting to solve this problem nationally through ad hoc fixed location-code additions will add complexity to a system whose greatest value is its simplicity, reliability, and broad reach.

⁶⁷ Further Notice at ¶ 71.

First, we join with DAS and the State Broadcasters Associations in support of a voluntary approach to the use of EAS symbols.⁶⁸ We understand that the insertion and storage of symbols may be possible through a manufacturer-created software update to existing EAS devices, and that providing symbols is likely possible for most television stations. Television stations broadcasting in the current ATSC 1.0 system would have to proactively add the symbol, like the process followed when a TV station chooses to show a radar weather map or bug during regular non-newscast programming. This may or may not be an automated system, so stations should have the flexibility to include the symbols consistent with their resources and the emergency at hand. ATSC 3.0 television stations would be able to more readily use symbols and may provide some presentation flexibility through the Advanced Emergency Information and Broadcast Application capability in NextGen TV sets.

For some radio stations, the challenges to providing symbols may outweigh the benefits. A radio station's EAS system would have to generate a JPEG file that may not integrate smoothly into a radio station's operation, the cost of which is uncertain. In addition, the presentation of the symbol on a consumer's radio would be highly dependent on the receiver's capability. For example, the resolution of symbols may have to be low to enable presentation on a dashboard in a car's HD Radio or hybrid (over-the-air plus internet) receiver. NAB thus submits that the FCC should allow, but not require, EAS Participants the option to use symbols based on their medium and resources.

⁶⁸ Reply Comments of DAS, PS Docket No. 25-224 (Nov. 13, 2025), at 3; Joint Reply Comments of the State Broadcasters Associations, PS Docket No. 25-224 (Nov. 13, 2025), at 8-11.

Second, for stations that choose to display EAS symbols, we believe that broadcasters should maintain control over how EAS symbols should be presented, including where they should be located, what size they should be, whether symbols should be transparent so as not to obscure other content, and how long they should appear.⁶⁹ These are matters best left to the editorial judgment of local broadcasters who are most familiar with the needs and interests of their communities, and how best to present emergency information during regular programming. For example, some stations may want to display a symbol in a corner of the screen, while others may prefer to place it at the bottom before or after the scrolled EAS message. Similarly, some stations may want to display the symbol for the entire length of an emergency, while others may want to show it only during the length of the EAS message to avoid obscuring more comprehensive emergency information on the screen.⁷⁰

⁶⁹ Further Notice at ¶ 80.

⁷⁰ NAB is agnostic as to what specific set of standardized symbols should be integrated, although we believe that using the same or similar symbols for both EAS and WEA would enhance public familiarity and comprehension of the symbols. *Id.* at ¶¶ 79-80.

V. CONCLUSION

For the reasons stated above, NAB supports the Commission's proposals in the Further Notice, subject to the concerns and conditions discussed above. We appreciate the FCC's ongoing efforts to enhance EAS and look forward to working with the FCC and other stakeholders on implementation of the various proposals.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Rick Kaplan".

Rick Kaplan
Larry Walke
David Layer
Kelly Williams

National Association of Broadcasters
1 M Street, S.E.
Washington, D.C. 20003
(202) 429-5430

August 29, 2026