

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	)	

REPLY COMMENTS OF THE
NATIONAL ASSOCIATION OF BROADCASTERS

September 29, 2026

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY.....	1
II.	THE RECORD SUPPORTS A FLEXIBLE, CONTROLLED SOFTWARE EAS APPROACH	4
A.	Commenters Endorse the Potential Benefits of Allowing the Use of EAS Software	4
B.	The FCC Should Preserve EAS Resiliency Without Mandating a Particular Location ...	5
C.	The FCC Should Adopt a Reasonable Middle Ground Approach to Regulating a Software-Based EAS Model.....	7
D.	Existing Cybersecurity Requirements Combined with EAS Software Operating in a Controlled, Secure Environment Will Address Cybersecurity Risks.....	9
E.	The FCC Should Retain the Existing 60-Day Repair Period for EAS Software Until it Can Establish a New Policy Based on Real-World Experience	10
III.	THE RECORD SUPPORTS AN INCREMENTAL APPROACH TO MODERNIZING EAS	12
A.	The FCC Should Require Authentication of CAP Alerts While Proceeding Cautiously with Legacy EAS	12
B.	A Universal Alert Identifier Could Enhance EAS if Implemented Without Adding Unnecessary Burdens	14
C.	The Commission Should Allow Enhanced Geotargeting of CAP Alerts While Recognizing the Limits of Legacy EAS.....	15
D.	The FCC Should Promote, But Not Require, the Use of EAS Alert Symbols	17
IV.	CONCLUSION	18

**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	)	

**REPLY COMMENTS OF
THE NATIONAL ASSOCIATION OF BROADCASTERS**

I. INTRODUCTION AND SUMMARY

The National Association of Broadcasters (NAB)¹ hereby submits reply comments on the above-captioned Further Notice of Proposed Rulemaking, in which the Commission proposes certain steps to modernize the Emergency Alert System (EAS).² We join with the vast majority of commenters that support the FCC's grant of NAB's Petition for Rulemaking seeking rules changes to allow EAS Participants to use a software-based approach to process EAS messages.³ The National Weather Service (NWS), state emergency managers, a

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, Protecting the Nation's Communications Systems from Cybersecurity Threats, Wireless Emergency Alerts, Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System*, 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).

³ 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).

leading EAS manufacturer, accessibility representatives, and EAS Participants⁴ all agree that providing this voluntary option would enhance the effectiveness of EAS.⁵ NAB also appreciates that DAS, which previously labeled our Petition “premature and procedurally inappropriate,”⁶ now offers thoughtful suggestions for implementing a software EAS model.⁷ We have discussed this issue with DAS on multiple occasions in 2026 (including most recently on September 9th) and although we respectfully disagree with many of its suggestions, we look forward to continued collaboration. Thus, the question is no longer whether the FCC should move forward with allowing a software-based EAS model, but how best to implement the option.

⁴ Comments of National Weather Service, PS Docket Nos. 15-94, 15-91, 22-329, 25-224 (Aug. 31, 2026), at 3; Comments of The City of New York’s Emergency Management Department (NYCEM), PS Docket Nos. 15-94, 15-91, 22-329, 25-224 (Aug. 31, 2026), at 10-11; Comments of Michigan State Police Emergency Management and Homeland Security Division, PS Docket Nos. 15-94, 15-91, 22-329, 25-224 (Aug. 31, 2026), at 3; Comments of the Washington Emergency Management Division (WEMD), PS Docket Nos. 15-94, 15-91, 22-329, 25-224 (Aug. 31, 2026), at 3; Comments of Sage Alerting Systems, Inc., PS Docket Nos. 15-94, 15-91, 25-224 (Aug. 31, 2026), at 2; Comments of American Council of the Blind, American Foundation for the Blind, and Bridge Multimedia Corporation (ACB et al.), PS Docket Nos. 15-94, 15-91, 25-224 (Aug. 31, 2026), at 14-15; Comments of NAB, PS Docket Nos. 15-94, 15-91, 22-329, 25-224 (Aug. 31, 2026), at 3-12; Comments of New York Public Radio (NYPR), PS Docket Nos. 15-94, 15-91, 22-329, 25-224 (Aug. 31, 2026), at 1; Comments of iHeartMedia, Inc. (iHeart), PS Docket Nos. 15-94, 15-91, 25-224 (Aug. 31, 2026), at 2-6; Comments of America’s Public Television Stations and the Public Broadcasting Service (collectively PTV), PS Docket Nos. 15-94, 15-91, 25-224 (Aug. 31, 2026), at 4-8; Comments of NCTA – The Internet & Television Association (NCTA), PS Docket Nos. 15-94, 15-91, 25-224 (Aug. 31, 2026), at 3-5; Comments of America’s Communications Association – ACA Connects (ACA), PS Docket Nos. 15-94, 15-91, 25-224 (Aug. 31, 2026), at 5-6; Comments of Sirius XM Radio LLC, PS Docket Nos. 15-94, 15-91, 25-224 (Aug. 31, 2026), at 3-5; Comments of DIRECTV, LLC, PS Docket Nos. 15-94, 15-91, 25-224 (Aug. 31, 2026), at 4-5.

⁵ Further Notice at ¶¶ 88-96.

⁶ Comments of Digital Alert Systems, Inc. (DAS), PS Docket Nos. 15-94 and 22-329 (May 2, 2025), at 45.

⁷ Comments of DAS Part II, PS Docket Nos. 15-94, 15-91, 25-224 (Aug. 31, 2026), at 4-30. DAS filed two sets of comments; Part I covers the authentication, geotargeting and the other non-EAS software issues, and Part II discusses EAS software issue.

Commenters believes that testing and certification of EAS software through a process similar to that used for existing equipment would be appropriate,⁸ and opposes DAS's request to delay authorization until the FCC defines and mandates a broad "certification boundary" that could encompass a station's entire technology stack.⁹ Regarding security, we agree with the FCC that EAS software should not be "generated within cloud-based systems or cloud-based third-party EAS services."¹⁰ Any such risks should be mitigated by confining EAS software deployment to trusted, controlled, and secure environments,¹¹ combined with the FCC's new requirements for stronger passwords, prompt implementation of software patches, and firewalls or network segmentation.¹² Finally, the record opposes reducing the time period to repair or replace defective EAS software from 60 days to 72 hours;¹³ instead, the FCC should wait until it can create a new policy based on real-world experience with EAS software.¹⁴

Commenters support the FCC's proposals to improve the authentication and geotargeting of EAS, although some note technical challenges that dictate a cautious approach for legacy EAS alerts.¹⁵ NAB has no objections to use of a universal alert

⁸ Sage Comments at 12.

⁹ DAS Comments Part II at 6, 8, and 16. As the leading provider of EAS equipment, DAS offers a valuable perspective, but we would be remiss to ignore the possibility that DAS's push to defer authorization until the FCC's defines and requires extraordinarily broad testing and certification of EAS software may be colored by its concerns that permitting EAS software "would not affect all suppliers evenly." *Id.* at 29.

¹⁰ Further Notice at ¶ 98.

¹¹ NAB Comments at 13.

¹² Order at ¶¶ 18-27.

¹³ NYPR Comments at 5; ACB et al. Comments at 15; NCTA Comments at 5-6; ACA Comments at 6-7; Sage Comments at 15-16.

¹⁴ NAB Comments at 14-16.

¹⁵ NAB Comments at 17-18; DAS Comments Part II at 17-18 and 22-23; NCTA Comments at 2 (urging rejection of legacy EAS authentication); ACA Comments at 3 (same).

identification number to reduce duplicative alerts, and supports voluntary use of visual symbols to improve the understanding of EAS messages, if feasible.¹⁶ However, NAB again cautions the FCC against new mandates that could outstrip the capacity of existing EAS devices or force EAS Participants to purchase new EAS equipment.¹⁷

II. THE RECORD SUPPORTS A FLEXIBLE, CONTROLLED SOFTWARE EAS APPROACH

A. Commenters Endorse the Potential Benefits of Allowing the Use of EAS Software

Commenters support the FCC's plan to permit the voluntarily use of software to perform EAS functions instead of a dedicated physical device. Sage describes the option as moving EAS beyond its decades-old "custom hardware box solution" and into a modern architecture capable of improving "security, performance, redundancy, and manageability."¹⁸ iHeart notes that stations already use software-defined architectures throughout automation, audio processing, monitoring, networking, routing, and content distribution.¹⁹ Thus, software EAS would not be an untested departure, but a logical extension of technologies already used throughout the broadcast air chain.

First, keeping it optional means that no EAS Participant would be required to abandon their dedicated hardware EAS equipment. NAB expects that many broadcasters, especially smaller stations that rely on outside engineers and vendors for EAS support, will continue to use hardware boxes for many years, if not forever. But stations seeking to

¹⁶ PTV Comments at 10-11; NYCEM Comments at 2-3 and 7-8; DAS Comments Part I at 10-14 and 23-28; Comments of National Public Radio, Inc. (NPR), PS Docket Nos. 15-94, 15-91, 22-329, 25-224 (Aug. 31, 2026), at 8; Comments of TDI et al., PS Docket Nos. 15-94, 15-91, 22-329, 25-224 (Aug. 31, 2026), at 4-5; NWS Comments at 2.

¹⁷ NAB Comments at 3 and 19.

¹⁸ Sage Comments at 2.

¹⁹ iHeart Comments at 3-4; PTV Comments at 4-5 (voluntary software option could reduce participants' costs while increasing operational flexibility and system security).

operate more efficiently using software would no longer have to purchase and maintain an EAS box because the FCC's rules presume a hardware-based system.²⁰ Second, emergency managers and EAS Participants demonstrate that software will streamline maintenance, facilitate security updates,²¹ and improve overall system performance.²²

Third, software can enhance EAS redundancy by eliminating single points of failure and making it easier to provide backup EAS when the primary system becomes unavailable due to power failure, loss of Internet service, or lack of physical access.²³ Finally, the FCC expects software to better support advanced alerting functions, such as richer CAP content, geotargeting calculations, text-to-speech and speech-to-text capabilities, and delivery of CAP data over secondary channels or subcarriers.²⁴

B. The FCC Should Preserve EAS Resiliency Without Mandating a Particular Location

NAB agrees with the FCC that software EAS should not depend on real-time processing by a remote or third-party EAS service. However, while NAB initially agreed with the FCC that software EAS should be located at an EAS Participant's "local facility used to provide service" (e.g., a station studio or transmitter site, cable operator's headend) to reduce concerns that power outages or infrastructure damage may disrupt Internet connectivity and cut off EAS Participants from their EAS system,²⁵ the record shows that a "local facility" requirement may be impractical for some EAS Participants. PTV asserts that some statewide public television networks use centralized hub-and-spoke systems for which

²⁰ PTV Comments at 4-5; iHeart Comments at 5.

²¹ NYCEM Comments at 10-11; WMED Comments at 3.

²² iHeart Comments at 4-5; NYPR Comments at 3-4; ACA Comments at 5.

²³ Further Notice at ¶ 94; iHeart Comments at 4-5.

²⁴ Further Notice at ¶ 95; ACB et al. Comments at 15.

²⁵ Further Notice at ¶ 98; NAB Comments at 5-6..

locating EAS software at a staffed, redundant facility outside a station's service area may be more resilient than locating it at an isolated, unmanned transmitter site.²⁶ SiriusXM explains that its nationwide satellite architecture does not have the equivalent of a local broadcast studio or cable headend for every service area.²⁷ NCTA and ACA state that cable networks increasingly use IP-centric architectures that could be frozen in time by a mandate to locate software at a specific local site.²⁸

DAS states that EAS should not depend on a remote or cloud-based third-party EAS service, but would support remote monitoring, reporting, support, updates, and storage, so long as loss of Internet connectivity does not affect EAS performance.²⁹ Sage states that a categorical exclusion of "cloud-based systems" is too imprecise because the term can describe not only remote third-party computing, but also virtualized computing resources operating on hardware controlled by an EAS Participant. Sage suggests prohibiting EAS functions performed using third-party computing or storage resources instead of broadly excluding anything described as "cloud-based."³⁰

Thus, although "local facility" implementation of EAS software may work for many broadcast stations, NAB now understands that the better approach would be to focus on EAS reliability if physical access or Internet connectivity is unavailable. The FCC should accommodate architecture varieties provided an EAS Participant maintains control over EAS and can ensure continued service during an emergency.

²⁶ PTV Comments at 7-8.

²⁷ Sirius XM Comments at 4-5.

²⁸ NCTA Comments at 4-5; ACA Comments at 5-6.

²⁹ DAS Comments Part II at 25-26.

³⁰ Sage Comments at 17-18.

C. The FCC Should Adopt a Reasonable Middle Ground Approach to Regulating a Software-Based EAS Model

Commenters agree that EAS software must be reliable, secure, and subject to appropriate testing and oversight, although differ on how broadly the FCC should define a software-based model for purposes of regulation. On one hand, DAS supports testing EAS software as part of a complete “EAS Implementation” with a so-called “certification boundary” that could encompass not only EAS software and host, but an EAS Participant’s entire “operating system, interfaces, dependencies, deployment topology, and security controls,”³¹ all the way down to a station’s “automation system, routers, A/V processors, playout systems, transport encoders, multiplexers, importers/exporters, broadcast payload generation systems, or potentially . . . generic PCs.”³²

NAB understands DAS’s concerns underlying this approach and agrees that a poorly managed software environment could affect EAS reliability. We also appreciate the public safety nature of EAS that might warrant heightened attention. But those concerns do not justify including such a large, ever-changing collection of non-EAS systems components within the testing boundary for a software-based EAS model. DAS itself concedes that the certification, recovery, and accountability obligations of its approach would be substantial and likely to add cost to an EAS Participant’s IT environment.³³ DAS’s proposed regime could essentially require a different version of the same hardware-based approach required under the existing rules, except with a much larger universe of systems and components subject to

³¹ DAS Comments Part II at 23.

³² *Id.* at 8.

³³ *Id.* at 19-20.

the FCC's EAS rules. All this additional regulation would also negate most of the potential benefits and flexibility of EAS software sought by the FCC and other stakeholders.

On the other hand, NCTA and ACA urge the FCC to "avoid" certification requirements for EAS software because Part 2 tests for unintentional radiators rather than EAS functionality. NCTA states that software-specific certification is unnecessary because EAS functionality will be ensured by the existing rules in Part 11 and FEMA IPAWS requirements.³⁴ This approach would be expedient, but NAB has qualms that it may not provide enough assurance for software that must provide mandatory public warnings.

NAB supports a middle-ground approach.³⁵ EAS software should not be an uncontrolled application that can be installed on any generic PC without regard to security or interoperability.³⁶ But neither should the FCC require certification of a broadcaster's entire operation, including non-EAS elements. Rather, the certification framework used for existing EAS hardware devices should be adapted to software, including review by a telecommunications certification body or comparable entity, or self-certification by providers that follow cybersecurity best practices,³⁷ government oversight, and required testing.

EAS software will perform the same fundamental Part 11 functions as the software already housed inside physical devices, and moving those functions outside such devices

³⁴ NCTA Comments at 5-6; see *also* ACA Comments at 5-6 (opposing application of Part 2 certification process to EAS software in favor of reliance on Part 11 requirements, vendor testing, and documentation.)

³⁵ NYPR Comments at 4-5 (supporting certification of EAS software while urging the FCC to regulate "with a light touch" and preserve deployment flexibility); PTV Comments at 4 (supporting "rigorous" certification); ACB et. al Comments at 14-15 (supporting technology-neutral flexibility for EAS software).

³⁶ NAB Comments at 6; see *also* Sage Comments at 2-3 (rejecting a model in which EAS software is sold as a downloadable package, downloadable to any computer, and the EAS Participant is responsible for security and interoperability).

³⁷ NAB Comments at 8-11.

does not change the requirements of EAS.³⁸ Therefore, testing and certification of software EAS should follow the same general standards as standalone hardware systems, under appropriately adapted sections of Parts 11 and 2 of the rules, without expanding coverage to every component of a broadcast facility. The FCC adopts essentially this approach in Appendix B of the Further Notice, consistent with its goal to remove unnecessary regulatory barriers to modernizing the nation’s public alerting systems.³⁹

D. The FCC’s New Requirements Combined with EAS Software Operating in a Controlled, Secure Environment Will Address Cybersecurity Risks

Cybersecurity must be an integral part of any software-based EAS framework; however, NAB believes the far-reaching approach recommended by DAS is unnecessary. Like its arguments for an expansive “certification boundary,” DAS seeks to encompass within a sort of cybersecurity boundary extensive logging, auditing, and management of an EAS software platform, various configurations, access controls, network segmentation and interfaces, and almost every component of a broadcaster’s operation.⁴⁰ NAB agrees that EAS providers should follow security best practices, but DAS’s approach would effectively create an almost boundless cybersecurity regime for a broadcaster’s IT infrastructure.

Also, DAS’s recommendation is inconsistent with the FCC’s approach to cybersecurity in the Order, in which it specifically declined to impose a broad cybersecurity risk management framework on EAS Participants. Instead, the FCC adopted targeted EAS safeguards requiring stronger passwords, prompt software patching, and sturdier firewalls or comparable network segmentation for EAS equipment.⁴¹ It would be illogical for the FCC to

³⁸ *Id.*; NAB Comments at 9-11.

³⁹ Further Notice at ¶ 87 and Appendix B.

⁴⁰ DAS Comments Part II at 14-19.

⁴¹ Order at ¶¶ 13-27.

reject an all-encompassing cybersecurity regime in the Order but adopt DAS's proposal that would essentially recreate such a regime as a condition of authorizing software EAS.

Again, NAB contemplates a model consisting of tested EAS software operating on trusted hardware in a supported and secure environment – not an uncontrolled application that is exposed directly to the public Internet.⁴² Broadcasters are familiar with protecting their existing EAS equipment from cyber problems, and believe that a properly managed implementation of EAS software would present essentially the same risks and use the same mitigation measures.⁴³ We also observe that an important advantage of software is the ability to rapidly address security vulnerabilities through software patches and remote updates instead of having to manually update or ship a box to a vendor.⁴⁴

E. The FCC Should Retain the Existing 60-Day Repair Period for EAS Software Until it Can Establish a New Policy Based on Real-World Experience

The FCC proposed reducing from 60 days to 72 hours the period for repairing or replacing defective EAS software. The FCC based this change partly on a premise that software defects should usually be more quickly reparable through a remote fix.⁴⁵ The Commission also suggests that EAS software may be more prone to cyberattacks because of its IP exposure, increasing the need for the Commission's awareness of software issues.⁴⁶ However, the record demonstrates that neither reason supports a 72-hour deadline. There are too many uncertainties regarding how software-based EAS will be implemented and supported to substantially shorten this repair deadline before the technology has even been

⁴² NAB Comments at 12-14.

⁴³ Sage Comments at 15.

⁴⁴ NAB Comments at 12-13; see also ACA Comments at 5-6.

⁴⁵ Further Notice at ¶ 114.

⁴⁶ *Id.*

implemented, and the proposed 72-hour deadline may rest on an overly simple view of the problems that may affect EAS software functionality.⁴⁷

EAS vendors explain that few problems at an EAS installation are likely to result from a software bug that can simply be remedied through a software update.⁴⁸ First, EAS software would operate on some kind of hardware platform, so if a problem is hardware-related, the time needed for repair will be no different than now.⁴⁹ Also, like existing devices, software failures could involve other parts of a participant's operating system that often take longer than 72 hours to repair, such as "network addressing, AoIP channel changes, interface to automation systems, email addresses, firewall settings, and similar issues that affect all broadcast equipment."⁵⁰ In addition, cybersecurity-related problems can be more complicated because detection, investigation, and repair can involve multiple implementations and vendors.⁵¹ Finally, Sage notes that, for stations that rely on outside engineers, it will "often take more than 72 hours to schedule an on-site support visit."⁵²

Nor should the FCC shorten the repair time based on an assumption that EAS software is uniquely vulnerable to cybersecurity problems. Sage disputes the idea that software would have a larger cyber-attack surface than hardware, since existing EAS boxes already have APIs, remote access points, and other potential attack points.⁵³ A properly managed software system should have the same risks and mitigation paths as hardware

⁴⁷ NAB Comments at 14-16.

⁴⁸ Sage Comments at 15; DAS Comments Part II at 20.

⁴⁹ Sage Comments at 15.

⁵⁰ *Id.*

⁵¹ *Id.*; DAS II Comments at 20.

⁵² Sage Comments at 16.

⁵³ *Id.*

devices.⁵⁴ Accordingly, NAB submit that the FCC should “keep the current 60-day rule,”⁵⁵ at least until it can establish a new policy based on real-world experience with EAS software.

III. THE RECORD SUPPORTS AN INCREMENTAL APPROACH TO MODERNIZING EAS

NAB supports consideration of ways to improve the authentication and geotargeting of alerts, as well as the use of universal identifiers and symbols, provided allowances are made for the hurdles to implementation in the legacy EAS environment.

A. The FCC Should Require Authentication of CAP Alerts While Proceeding Cautiously with Legacy EAS

Commenters support the FCC’s proposal to require EAS Participants to reject CAP messages that do not contain a valid digital signature,⁵⁶ noting that authentication of CAP-based alerts is already routine in IPAWS, in which alerts are digitally signed and EAS equipment validates the signature.⁵⁷ This is a straightforward way to close a security gap and prevent spoofed alerts.⁵⁸ Sage would require a valid signature for any CAP message, and explains that validation information could be preloaded so validation need not depend on Internet access.⁵⁹ NAB has no objections, but reiterates our request for a phased implementation and the need for tailored guidance from the FCC or FEMA/IPAWS about how broadcasters should handle digital signatures.⁶⁰

⁵⁴ *Id.* at 16.

⁵⁵ *Id.*

⁵⁶ Further Notice at ¶¶ 41-42.

⁵⁷ *Id.* at ¶¶ 43-44 (noting that more than 2,000 federal, state, local, tribal, and territorial alerting authorities use IPAWS and that only 23 of the 20,682 EAS Participants in the 2023 nationwide test reported CAP digital-signature problems).

⁵⁸ NYCEM Comments at 1-2; Cal OES Comments at 2; NCTA Comments at 2; AWARN Comments at 2.

⁵⁹ Sage Comments at 3-4.

⁶⁰ NAB Comments at 17.

Authenticating legacy EAS messages is more complex. Unlike CAP, the legacy EAS Protocol was not designed to carry authentication information and is severely limited in the amount of data it can transmit, so that adding digital signature data would lengthen and delay transmission of alerts.⁶¹ The FCC also noted questions about relying on the Internet to check for encryption key certificates, encryption key management, and interoperability with existing consumer equipment.⁶²

NWS stresses that it “cannot digitally sign our EAS messages via NWR at this time,” and further explains that inserting authentication data could force removal of part of its EAS message used to activate some National Weather Radio (NWR) receivers to receive alerts, thereby degrading NWR alerting quality.⁶³ These are major hurdles because NWS triggers the vast majority of EAS alerts. Thus, unless NWS legacy alerts can be authenticated, the benefits of authenticating legacy messages would be severely limited.⁶⁴

Sage offers an approach to authenticating legacy alerts using a pre-stored public key, but notes important drawbacks regarding the length of EAS transmissions, potentially missed alerts, and compatibility problems with NWR alerts.⁶⁵ DAS proposes to add a short supplemental data block (EAS Data Extension or EDX) that carries authentication data for a legacy EAS alert instead of trying to include the data inside the legacy EAS header, but also notes this would lengthen EAS transmissions by 4 to 4 ½ seconds.⁶⁶

⁶¹ Further Notice at ¶ 45.

⁶² *Id.* at ¶ 46 citing CSRIC VI, Final Report—Security Aspects of Emergency Alerting System (EAS) at 26-29 (2018), <https://www.fcc.gov/file/14853/download>.

⁶³ NWS Comments at 1.

⁶⁴ NAB Comments at 10-11; Sage Comments at 6.

⁶⁵ Sage Comments at 5-6.

⁶⁶ DAS Comments Part I at 10-11. AWARN suggests a similar concept involving a “purpose-built mechanism using a compact digital signature, while recognizing that NWS would require a transition period.

Thus, authenticating legacy alerts may be technically feasible, but the record does not yet support a mandate.⁶⁷ Before moving forward, the FCC should resolve questions related to testing, interoperability, compatibility with NWS alerts, length and delay of transmissions, costs to broadcasters.

B. A Universal Alert Identifier Could Enhance EAS if Implemented Without Adding Unnecessary Burdens

NAB members report that a universal alert identifier would not resolve the fairly uncommon instances when broadcasters relay duplicative alerts, such as when a station receives a CAP alert and a legacy alert about the same situation that has been slightly modified by the LP station it monitors, or when a station airs duplicate alerts from overlapping broadcasting signals.⁶⁸ But we recognize that alert originators and other commenters believe that a universal alert message ID could help prevent other kinds of duplicate alerts. They state that an identifier could help officials distinguish between an original alert, a duplicate transmission, and an update,⁶⁹ and help prevent public confusion or reduced confidence in EAS,⁷⁰

Given these benefits, NAB would not object to the creation of a universal alert identifier, under certain conditions. First, it should be developed by FEMA/IPAWS and stakeholders instead of creating a new station-side process.⁷¹ Second, the identifier should build on existing CAP capabilities and remain as an alert moves between CAP and legacy

⁶⁷ NCTA Comments at 3.

⁶⁸ NAB Comments at 18-19.

⁶⁹ WEMD Comments at 1; see *also* Comments of California Governor's Office of Emergency Services, PS Docket No. 25-22 (Aug. 29, 2026), at 2.

⁷⁰ NYCEM Comments at 2-3.

⁷¹ NAB Comments at 18-19; NWS Comments at 2; NYCEM Comments at 3.

paths.⁷² This would allow broadcasters to receive an identifier automatically within the existing EAS workflow, without having to shoulder any new responsibilities for creating, modifying, or managing identifiers and without requiring the replacement of existing equipment.⁷³ Finally, the universal identifier must clearly distinguish a genuine duplicate from an update, correction, cancellation, or other material change.⁷⁴

C. The Commission Should Allow Enhanced Geotargeting of CAP Alerts While Recognizing the Limits of Legacy EAS

NAB supports the FCC's aim to improve the geotargeting of EAS alerts, and its proposal to permit, but not require, EAS Participants to use the circles and polygons contained in CAP messages when deciding whether to transmit an alert.⁷⁵ This will provide better information than the basic county level codes now used and help prevent alerting audiences outside the area affected by an emergency. Emergencies usually do not follow county boundaries, and more precise targeting could reduce over-alerting and alert fatigue, particularly regarding emergencies that are confined to small areas.⁷⁶ NWS would go so far as to require EAS Participants to use polygons and circles when available.⁷⁷

NAB respectfully opposes this request.⁷⁸ Broadcasters should retain the editorial discretion to decide whether and where to transmit (non-Presidential) alerts, based on their familiarity with the needs, interests, and geography of their local community and their particular signal strength and coverage area. We also note that the protocol used for legacy

⁷² DAS Comments at 8.

⁷³ NAB Comments at 19.

⁷⁴ *Id.*

⁷⁵ Further Notice at ¶¶ 70-71; NAB Comments at 19-21.

⁷⁶ WEMD Comments at 2; Austin Comments at 2; San Mateo Comments at 1-3.

⁷⁷ NWS Comments at 2-3.

⁷⁸ NPR Comments at 8.

EAS is organized around county-level codes rather than circles and polygons. Unlike mobile devices that receive WEA alerts, radio and television receivers do not know their own geographic location, so an EAS alert that is broadcast by a radio or TV station reaches all the receivers throughout a station's service area, and not just receivers inside a particular circle or polygon.⁷⁹ AWARN calls this a "cannon ball" approach, designed to reach a broad area -- as far as 60 miles from a station's transmitter -- depending on "topography, signal strength, and the location of receiving antenna[s]."⁸⁰

Requiring the use of codes that target smaller areas, like partial county alert (PCA) codes, will not make radio and TV receivers more location-aware and instead will add complexity and cost to the legacy EAS system, whose principal strengths are simplicity, reliability, and broad reach.⁸¹ For these reasons, NAB maintains our support for allowing the circles and polygons to inform decisions whether to relay CAP-based alerts, but oppose any mandate to use of PCA codes or other geotargeting mechanisms in legacy EAS.

Finally, we highlight the potential of ATSC 3.0 to support enhanced alert geotargeting. Unlike conventional television receivers, ATSC 3.0- configured receivers can be location aware by comparing their location with a polygon or circle within the alert and determine whether the message applies to that receiver.⁸² AWARN adds that Advanced Emergency Information ("AEI") can be sent along with a broadcast signal and supplement emergency information with maps and richer data.⁸³ Importantly, however, the ability to use AEI is not

⁷⁹ DAS Comments Part I at 21-22.

⁸⁰ AWARN Comments at 3.

⁸¹ NAB Comments at 20-21; DAS Comments Part I at 22-23.

⁸² Sinclair Comments at 3.

⁸³ *Id.* at 3-4; AWARN Comments at 3.

built into the hardware of receivers, so AWARN advocates for voluntary use of those capabilities as a way to complement, but not replace, EAS.⁸⁴

D. The FCC Should Promote, But Not Require, the Use of EAS Alert Symbols

NAB appreciates the accessibility and public safety benefits that symbols could provide. IDE explains that a symbol can help viewers more quickly identify the type of danger conveyed by an alert.⁸⁵ TDI et al. agree, but emphasize that symbols should supplement rather than replace accessible emergency information.⁸⁶ NYAG et al. support standardized symbology because visual elements could assist people with disabilities, limited literacy, or limited English proficiency, but caution that introducing unfamiliar symbols too quickly may cause confusion.³ They emphasize the importance of public education and the ongoing presentation of the underlying information in an EAS message.⁸⁷

NAB agrees that accessibility should be central to the development of any symbol set and that symbols should supplement, but not replace, the text and audio in an EAS message needed to convey an actionable warning. Thus, we continue to support creation of a common set of symbols, and encourage the FCC to “permit and encourage, but not require” their use.⁸⁸

Finally, voluntary use of symbols should preserve broadcasters’ editorial control over how symbols are presented. Broadcasters are best positioned to determine where a symbol should appear, its appropriate size and duration, and how it should interact with captions,

⁸⁴ AWARN Comments at 3.

⁸⁵ Comments of International Deaf Emergency (IDE), PS Docket Nos. 15-91, 15-94, and No. 25-224 (Aug. 31, 2026), at 4-6.

⁸⁶ TDI et al. Comments at 4-6.

⁸⁷ Comments of Attorneys General of New York et al. (NYAG et al.), PS Docket Nos. 15-91, 15-94 and 25-224 (Aug. 31, 2026), at 5-8.

⁸⁸ AWARN Comments at 3-4; NAB Comments at 22-23; PTV Comments at 10-11; .

crawls, maps, and other on-screen content.⁸⁹ We note that this approach is consistent with accessibility commenters, such as IDE, which the accessibility concerns raised in the record rather than contrary to them. IDE, which cautions that symbols should not obscure captions, sign-language content, or essential programming information.⁹⁰

IV. CONCLUSION

NAB supports the Commission's proposals in the Further Notice, subject to the views and caveats described above. We look forward to continued partnership with the FCC and other stakeholders on efforts to improve EAS.

Respectfully submitted,

**NATIONAL ASSOCIATION OF
BROADCASTERS**

1 M St. SE
Washington, DC 20003
(202) 429-5430



Rick Kaplan
Larry Walke

David Layer
Kelly Williams
Industry Affairs and Innovation

September 29, 2026

⁸⁹ NAB Comments at 22-23.

⁹⁰ IDE Comments at 5-6.