Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Amendment of Part 11 of the Commission's Rules	)	PS Docket No. 15-94
Regarding the Emergency Alert System	)	
	)	
Wireless Emergency Alerts	)	PS Docket No. 15-91

COMMENTS OF
THE NATIONAL ASSOCIATION OF BROADCASTERS

National Association of Broadcasters
1771 N Street N.W.
Washington, D.C. 20036
(202) 429-5430

Kelly Williams
NAB Technology

Rick Kaplan
Larry Walke

June 8, 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Local broadcasters are the backbone of the nation's Emergency Alert System (EAS), as our ability to reliably reach virtually all Americans plays an indispensable role in the dissemination of EAS alerts. We take this responsibility seriously, and support continued improvement to the system. NAB applauds the Commission for its forethought in launching this proceeding regarding a new EAS paradigm, and appreciates this opportunity to comment on the various proposals raised in the Notice.

As a preliminary matter, NAB respectfully refrains from providing initial comment on the proposed streamlining and contents of state EAS plans. For the time being, NAB will defer to the expertise of State Emergency Communications Committee (SECCs) members who prepare such plans. We believe that SECCs, as well as state broadcasting associations, state emergency managers and other local stakeholders can offer the most useful guidance for creating an efficient online process for state EAS plans, and the appropriate contents of such plans.

Regarding enhanced EAS testing and public awareness, NAB urges the Commission to avoid micromanagement of local efforts. For example, instead of mandating the frequency and parameters of EAS tests, the Commission should simply provide local EAS stakeholders with the tools they need to conduct such tests, and then allow them the discretion to schedule and structure EAS tests consistent with the characteristics of the local population, geography and weather. Local emergency managers and SECCs are best positioned to decide how often to conduct live code EAS tests, or whether such tests are even necessary. Similarly, the Commission should not dictate whether EAS public service campaigns must include the live code, especially given the risks of triggering false alerts or mistakenly causing public confusion.

NAB is gratified the Commission appears poised to modernize its rules permitting cable television providers to unilaterally force-tune broadcasters to another cable channel during EAS events. We have long urged the Commission to recognize the folly of allowing cable operators to interrupt viewers' access to the comprehensive and often life-saving emergency news provided by television broadcasters, in favor of some designated cable channel that displays the barebones EAS message. It is our understanding that technology advances have rendered cable operators' objections to updating this rule largely moot, given that some cable operators have successfully implemented selective override or other process that maintains access to broadcast stations. We believe that if some cable systems can manage this change, others can too, if the Commission acts.

NAB supports wider dissemination of multilingual EAS alerts, and welcomes the recent experiment in Minnesota as a successful first step. However, we note that broadcasters still function primarily as passive conduits of EAS alerts that are originated and issued by emergency managers, and for the near future, should not be required to translate EAS alerts at the station level. Only a few months ago, the Commission found that alert originators are best positioned to effect multilingual alerting because broadcasters lack the capability, and this view remains correct. Machine-generated EAS alert translation is still a nascent technology, such that a premature mandate could diminish the accuracy, uniformity, and timeliness of EAS alerts. Therefore, use of machine-generated EAS alerts should remain voluntary, at least until such time the necessary technology is fully mature and unfailing.

Broadcasters are committed to safeguarding EAS. However, given the increasing cybersecurity risk to all IP-based communications systems, NAB supports the Commission's efforts to enhance the security of EAS. Specifically, we agree that EAS Participants should be

required to demonstrate efforts to address EAS security based on industry best practices or reasonable alternative means. However, certain parts of the Commission's approach may be unduly burdensome. For example, requiring an annual certification of EAS security as part of the new Electronic Test Reporting System (ETRS) underestimates the resources needed to perform a complete, accurate technical review of a station's equipment and systems. Most broadcasters would have to hire an outside IT consultant to fulfill this obligation. A formal certification would also be subject broadcasters to potential Commission enforcement, which seems to contradict the Commission's goal of allowing EAS Participants the flexibility to address EAS security as they see fit. Instead, the wiser course is to incorporate the recommended EAS security measures into the Commission's Self-Inspection Checklists, and treat compliance like similar obligations imposed on broadcasters concerning the operational status of EAS equipment.

We are further concerned that broadcasters will be unable to research, complete and file a report about a false EAS alert within thirty minutes of such an alert, as proposed in the Notice. In many cases, thirty minutes will not allow stations to figure out the nature of a false alert, leading to incomplete or mistaken filings. Even more troublesome is the proposal to make public the filing of such reports, which may needlessly embarrass stations. NAB can discern no reason for an initial false alert report to be made public. Thus, the filing of such a report should be treated as presumptively confidential.

NAB generally supports enhancing the authentication of EAS messages. Although we are agnostic on how best to achieve improved authentication, we caution the Commission to consider the implications of any new mechanisms on consumer response to EAS alerts, and how to include authentication for alerts issued by the National Weather Service NOAA Weather Radio System. Most importantly, NAB urges the Commission to allow a longer, more

flexible time frame for implementation of any authentication technology that might require the replacement of EAS equipment.

Finally, NAB offers a few observations concerning potential changes to the fundamental structure of EAS explored in the Notice. First, the Commission should avoid imposing any new obligations that would require broadcasters to purchase new EAS equipment. Second, the Commission should be wary of centralizing and virtualizing the EAS system in a way that produces a single point of failure. Third, one of the EAS system's most attractive features is ease-of-use. Virtualization and similar changes could overly complicate the system, especially for smaller broadcasters and other EAS Participants with few IT resources. Finally, for the time being, NAB supports retaining the dual pathways provided by the legacy analog EAS system and the IP-based CAP-formatted IPAWS system. The two systems are complementary and provide critical redundancy, particularly during emergencies that disrupt Internet access.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Amendment of Part 11 of the Commission's Rules	)	PS Docket No. 15-94
Regarding the Emergency Alert System	)	
	)	
Wireless Emergency Alerts	)	PS Docket No. 15-91

COMMENTS OF THE NATIONAL ASSOCIATION OF BROADCASTERS

The National Association of Broadcasters (NAB)[1] submits comments on the above-captioned Notice of Proposed Rulemaking regarding the Emergency Alert System (EAS).[2] For over 60 years, EAS and its predecessors have been the primary outlet for the President to communicate with the public during emergencies,[3] and during that time local radio and television broadcasters have served as the backbone of the system. Broadcasters are particularly proud of their role in creating AMBER Alerts in 1996 and distributing alerts that have led to the recovery of more than 820 missing and abducted children.[4] In addition, broadcasters are First Informers, delivering timely, often life-saving information to their local communities, both over-the-air and through other platforms such as station websites and

[1] NAB is a nonprofit trade association that advocates on behalf of local radio and television stations and broadcast networks before Congress, the Federal Communications Commission and other federal agencies, and the courts.
[2] *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, Wireless Emergency Alerts*, PS Docket Nos. 15-94 and 15-91, Notice of Proposed Rulemaking, 31 FCC Rcd 594 (2016) (Notice).
[3] Comments of the New Jersey Broadcasters Association, EB Docket No. 04-296, at 2, (Mar. 12, 2010).
[4] AMBER: America's Missing: Broadcasting Emergency Response Alerts, http://www.missingkids.com/KeyFacts (last visited April 26, 2016).

mobile apps, and their extremely popular accounts on social media websites.[5] Given our ability to reach virtually all Americans – especially when other communications platforms fail – radio and television stations play an essential role in the distribution of public alerts and warnings, as well as important information before, during, and after an emergency.

I. Live Code EAS Testing and EAS Public Awareness Campaigns Should Remain Within the Discretion of Local SECCs and EAS Participants

The Commission plans to facilitate live code testing of EAS to allow State Emergency Communications Committees (SECCs) and local public safety authorities more opportunities to assess the system under conditions that mirror a real emergency. NAB supports additional EAS testing. For example, we worked closely with the Commission, FEMA and local officials to ensure the success of the national EAS test in 2011. NAB provided information and advice broadcasters in advance of the national exercise, and spearheaded a public awareness campaign to educate Americans about the test nature of the exercise.[6] National and local television newscasts and morning shows, and radio talk shows, discussed the test, helping to minimize public confusion. NAB also helped to create and distribute a variety of Public Service Announcements – in both English and Spanish -- that were aired thousands of times as the test approached.[7] In addition, NAB provides information to radio and TV stations about Required Weekly Tests (RWT), Required Monthly Tests (RMT), and special tests for tsunamis, tornados and other events that SECCs may conduct during local

[5] NAB Comments on Petition Filed by the Minority Media and Telecommunications Council Proposing Changes to the Emergency Alert System (EAS) Rules to Support Multilingual EAS and Emergency Information, EB Docket No. 04-295, at 2-4, (May 28, 2014).
[6] *Strengthening the Emergency Alert System (EAS): Lessons Learned from the Nationwide EAS Test*, Report, Public Safety and Homeland Security Bureau, FCC, at 9-10, (April 2013) (EAS Test Report).
[7] *Id.*, at 10.

emergency preparedness weeks. EAS testing to identify potential problems is the best way to help ensure the reliability of America's primary emergency warning system.

That said, some of the test-related proposals in the Notice raise concerns. The Commission asks whether it should limit the frequency of live code tests, or alternatively, require that SECCs conduct a certain minimum number of tests.[8] The answer to both questions is no. Although additional live code EAS testing can improve the system's effectiveness, only SECCs in coordination with local public safety authorities can determine whether the benefits of such tests may outweigh the costs. Only local stakeholders are familiar with the weather and geography of a market or region, enabling them to be decide if a live code test for tornados or hurricanes, for example, is appropriate. For example, annual live code testing for tsunamis has been deemed appropriate in Alaska,[9] while it may be more sensible to conduct earthquake EAS testing in California and tornado testing in the Midwest, and in other areas, no live code testing may be warranted.

In the same vein, the Commission asks whether more frequent live testing would help raise public awareness of EAS.[10] Only SECCs and local public safety can best discern how many such tests are needed to adequately educate the public. NAB will thus defer to the expertise of local stakeholders, but we understand that Required Monthly Tests and Required Weekly Tests may be sufficient for most Americans. We are concerned that too frequent EAS testing may cause public fatigue or confusion. There is simply no need for the Commission to specify any particular number of live code tests, nor impose any specific

[8] Notice, 31 FCC Rcd at 625-626.
[9] *Id*.
[10] *Id.*, 31 FCC Rcd at 625.

procedures on EAS Participants to prevent public confusion.[11] SECCs and EAS Participants are well-versed in conducting successful EAS tests. Commission involvement in such local matters will only complicate the efforts of SECCs to target EAS testing to their local communities. The wiser approach is for the Commission to merely provide SECCs and other local EAS stakeholders with the tools they need to assess the local public interest regarding EAS, and chart the most appropriate course.

NAB is similarly concerned that the proposed streamlined use of the alert Attention Signal in public service announcements (PSAs) could lead to unintentional problems.[12] Again, this may be a solution in search of a problem, since we do not perceive a lack of EAS unawareness among the American public. Moreover, the Attention Signal is designed to be intrusive, and making it easier for EAS Participants to broadcast PSAs that include the signal could increase annoyance with EAS and cause citizens to tune out actual alerts. NAB appreciates the success of the PSA campaign for wireless emergency alerts (WEAs) that included the WEA signal, which sound identical to the EAS Attention Signal.[13] However, that effort was designed to introduce the new concept and purpose of WEAs to the American public.

On the other hand, EAS is widely known and we are concerned that the perceived benefits of allowing EAS PSAs that include the actual Attention Signal and header codes may

---

[11] The Commission's rules define EAS Participants as radio broadcast stations, including AM, FM, and low-power FM stations; digital audio broadcasting stations, including digital AM, FM, and low-power FM stations; Class A television and low-power TV stations; television broadcast stations, including digital Class A and digital low-power TV stations; cable systems; wireline video systems; wireless cable systems; direct broadcast satellite service providers; and digital audio radio service providers. 47 C.F.R. § 11.11(a).

[12] Notice, 31 FCC Rcd at 626

[13] *See* Letter from Roger L. Stone. Assistant Administrator (Acting) National Continuity Programs, Federal Emergency Management Agency, to David Simpson, Chief, Public Safety and Homeland Security Bureau, FCC (dated Nov. 6, 2015).

be outweighed by the risks. First, use of the actual Attention Signal may cause needless public confusion as to whether a PSA is actually a real emergency.[14] Second, using the live code would substantially increase the risks of an EAS PSA triggering an actual EAS alert, and allowing that alert to propagate to other EAS Participants.[15] Finally, as mentioned, more EAS PSAs may lead to negative public reactions to actual emergency warnings. Promoting EAS PSAs will merely place broadcasters at increased risk for airing EAS tones that are misperceived by the public and could lead to unforeseen problems. NAB thus recommends that additional EAS PSAs should only be permitted under extremely stringent conditions.

The Commission also seeks comment on how to ensure that EAS tests are accessible to persons with limited English proficiency and individuals with disabilities.[16] The Commission asks whether live code EAS testing provides particular benefits to these communities, and whether it should take any particular steps to prevent public confusion.[17] NAB supports additional EAS testing that informs all segments of society. However, again we emphasize the local nature of EAS testing, and respectfully question the need for Commission involvement in this context. Providing local public safety, SECCs and local EAS

---

[14] Needless to say, this is the exact same risk cited by the Commission in enforcement actions against broadcasters that mistakenly transmit the EAS tones or a facsimile thereof. *Viacom, Inc., ESPN, Inc.*, File Nos. EB-IHD-13-00011468 and EB-IHD-13-00011476, Forfeiture Order, at 1, (Jan. 30, 2015) ("As many of the complaints about EAS abuse have said, misuse of the tones creates a "Cry Wolf" scenario, which risks desensitizing the public to the significance of the tones in a real emergency.").

[15] Again, this is the exact same concern the Commission relies upon when imposing fines against broadcasters for issuing a false, improperly coded EAS message. *iHeart Communications, Inc.*, File No. EB-IHD-15-00018252, Order, at 1, (May 19, 2015) ("The transmission of those EAN codes, in turn, engaged the EAS equipment of certain other EAS participants, ultimately causing a multi-state activation of the EAS. As a result, iHeart transmitted or caused the transmission of EAS tones in violation of statutory and regulatory prohibitions against such transmissions in the absence of an emergency or test of the system.").

[16] Notice, 31 FCC Rcd at 628.

[17] *Id*.

Participants with any needed tools to conduct EAS testing, and allowing them the flexibility to construct and implement EAS tests is the best way to ensure that local community needs are met.

The recent test conducted by FEMA, Twin Cities Public Television (tpt), and Emergency and Community Health Outreach (ECHO) provide an example. That exercise, which included the first transmission of a multilingual alert message by FEMA and the first use of multilingual alerting as part of a regional test, stemmed from efforts by the locally based tpt and ECHO.[18] These organizations recognized a need for additional EAS familiarity among new community members with limited English proficiency, and worked to design a test in cooperation with FEMA to address those needs. No federal mandate or procedures were needed to implement this successful test.

As the Commission notes, live code testing is often conducted during a larger educational effort, like a "Tornado Awareness Week."[19] Certainly the design of EAS tests within these campaigns is best left to the discretion and creativity of local stakeholders who are familiar with the particular characteristics of their community. ECHO's evaluation of its own best practices supports this approach. For example, ECHO's findings for how best to engage a local community in the development of standardize multilingual alerts for Hmong and Somali populations in Minnesota include: (1) familiarity with the characteristics, numbers and needs of the local population; (2) established trust with the local community; and (3) involvement of local community in decisions about the content, translation and

[18] Susan Ashworth, *IPAWS Completes First Bilingual Test*, RadioWorld, (Nov. 18, 2015), available at http://www.radioworld.com/article/ipaws-completes-first-bilingual-eas-test/277548.
[19] Notice, 31 FCC Rcd at 624-625.

delivery of emergency information.[20] These kind of efforts are best conducted by local stakeholders.

II. Cable Operators Should Not Be Permitted to Force-Tune Television Broadcast Stations that Participate in EAS

NAB appreciates the Commission's long overdue recognition of the problems caused by its rules that allow cable TV providers to fulfill their EAS obligations by unilaterally force-tuning every consumers' cable box to a designated channel that displays the required EAS message.[21] For over twenty years, we have repeatedly described the disservice to television viewers who are automatically switched away from a broadcaster's live, in-depth coverage of an impending or ongoing emergency in favor of a cable operator's blue screen that carries only the bare-bones EAS message slide or crawl.[22]

Television broadcasters provide critical news that may include live tracking of tornados, hurricanes, floods, fires, and other severe weather conditions, all of which is interrupted by forced-tuning, also known as cable override. Forced-tuning also disrupts critical public safety announcements, such as the status of power failures, industrial explosions, and bridge collapses. The emergency information broadcast by television stations helps Americans make critical decisions like whether to shelter-in-place or evacuate, how best to assist family, friends and neighbors in need, and whether to visit the store for essentials. Consider the all-too-common situation when a television station's

---

[20] *Real-Time Warnings and Alerts for Non English Speaking Communities Evaluation of Best Practices in Community Outreach and Engagement in the Minnesota Multi-Language Messaging Initiative*, Wilder Research, (July 2015) (ECHO Report), available at https://www.wilder.org/Wilder-Research/Publications/Studies/Forms/AllItems.aspx.

[21] Notice, 31 FCC Rcd at 630-632.

[22] *See, e.g.*, NAB Comments, EB Docket No. 04-296, at ii, (Aug. 14, 2014); NAB Comments, EB Docket No. 04-296, at 10-13, (Nov. 4, 2013); NAB Informal Comments, EB Docket No. 04-296, at 11-14, (filed May 17, 2010); Letter from Edward O. Fritts, President, NAB, to Reed Hundt, Chairman, FCC, (May 30, 1997); NAB Petition for Partial Reconsideration, FO Docket Nos. 91-301 and 91-171, (Jan. 27, 1994); NAB Comments, FO Docket Nos. 91-301 and 91-171, at 14-16, (Nov. 12, 1993).

meteorologist is providing timely, detailed reports (often street-by-street) on an approaching storm, only to be interrupted by a cable system's EAS alert. For instance, on Monday, March 18, 2013, NewsChannel 5 in Nashville, Tennessee, was airing detailed, up-to-the minute coverage on the path of a tornado with winds of 105 mph when the local cable operator suddenly force-turned viewers to a black slide that offered no information beyond the fact that the National Weather Service had issued a Tornado Warning."

Automatic cable overrides of broadcast programming also hinder the timely delivery of AMBER Alerts. The National Center for Missing & Exploited Children, which administers the AMBER Plan, has stated that force-tuning is disruptive:

> "Our work with the AMBER Alert system has made us well aware of the challenges with cable over-ride, whereby viewers' TV screens have been interrupted with a blue slate and a crawl that states the existence of an emergency but fails to describe the type of emergency or where to go for further details. This has confused and distressed many viewers as to what to do in these situations. Lack of information has been a problem with cable-overrides. Moreover, overrides frighten people. In light of these concerns, this provision [permitting cable overrides] should be eliminated, or alternatively, broadcasters should retain the right to selective override . . . ."[23]

NAB agrees. Cable EAS overrides cause consumer confusion, and can increase viewers' risks by depriving them of timely, detailed emergency information provided by television stations. Indeed, some broadcasters' programming was overridden even during the nationwide EAS test in 2011, when cable operators had ample warning and time to prepare their participation in the test.

The Commission's current EAS rules undermine the public interest in access to timely emergency information. The Commission should address this problem by requiring local cable operators to implement "selective override" so that certain channels can be

[23] Comments of the National Center for Missing & Exploited Children, EB Docket No. 04-296, at 10, (Oct. 29, 2004).

selectively omitted during a cable operator's automatic system-wide EAS interruption. Under the current rules, broadcasters may negotiate with cable operators to implement selective override for local broadcast channels,[24] but in far too many instances such negotiations are fruitless. Cable operators routinely claim an inability to implement selective override because of equipment constraints.

However, the technology to implement selective override has been available for some time, rendering cable TV's objections largely moot. In fact, while forced-tuning continues to be a problem nationwide, as evidenced by the Commission's inquiry, we observe that some cable operators have successfully corrected the problem. Indeed, NAB has been informed that the situation mentioned above in Tennessee has been resolved because the cable operator invested in updated equipment capable of selective override. Apparently, whether to implement selective override is ultimately a matter of money,[25] and given the life-saving potential of uninterrupted broadcast emergency news, NAB believes that alleviating this problem is well-worth the investment by cable operators.[26] If some cable operators can fix the problem, others should be able to do likewise. Simply put, there are no more obstacles to eliminating the dangers of EAS forced-tuning.

---

[24] 47 C.F.R. §§ 11.51(g)(4) and (h)(4).

[25] For some cable systems, the actual cost of implementing selective override may be nominal. In 2002, the American National Standards Institute (ANSI) adopted a cable industry standard that specifies the inclusion of "selective override" functionality in cable equipment. *See American National Standards Institute, (ANSI) J-STD-042-2007; Emergency Alert Messaging for Cable (2007)* at § 5 and § 7.4 (specifying the protocol for conveying to an STB a list of services (channels), called *exception service*s, for which an emergency alert event shall not apply). *See also id.*, note in § 8.3 (which specifically acknowledges that terrestrial broadcast channels provide emergency alert functions and that those channels can be identified so that the cable alerts do not apply when STBs are tuned to those channels).

[26] NAB would not object to a more flexible regime for very small cable operators, such as these serving fewer than 5,000 subscribers. Notice, 31 FCC Rcd at 631. It may be unduly burdensome for some very small cable operators to implement selective override. For these entities, the Commission could consider a waiver process that allows cable operator to demonstrate financial hardship and seek additional time to comply with any new requirement.

The time for Commission action is now. There is simply no need to force-tune broadcast stations that participate in the EAS system. These stations receive and broadcast the exact same EAS message content that the cable operator provides on its designated channel, without interrupting the television station's live, detailed emergency news. If a television station is carrying the EAS warning, cable operators should be prohibited from switching away from that channel during an EAS event. Such an approach will provide certainty to broadcasters and viewers, without impeding the cable operator's ability to override other channels that do not participate in EAS.

III. Machine-Generated EAS Translation Should Remain a Voluntary Mechanism Until Reliable Technology is Available

The Commission seeks comment on the state of technology that can translate and provide EAS messages in non-English languages.[27] As discussed in the Notice, the joint tpt/ECHO project in Minnesota included the first transmission of a multilingual alert message by FEMA and the first use of multilingual alerting as part of a regional test.[28] Local broadcasters fully support wider dissemination of EAS alerts to non-English speakers, and welcome this project as a successful first step towards efficient, reliable machine-generated EAS translations. Nevertheless, multilingual alerting must remain voluntary at the EAS Participant level. Local broadcasters are passive participants in the EAS system, functioning essentially as conduits of messages crafted and issued by EAS alert originators.[29] Broadcasters employ EAS equipment that monitor other stations or sources for EAS warnings, and then automatically relays those messages to the public. NAB has noted that

[27] Notice, 31 FCC Rcd at 636-637.
[28] *Id.*, 31 FCC Rcd at 627-628.
[29] EAS Test Report at 10.

the passive nature of the EAS process enhances the reliability and consistency of the entire system, which disseminates uniform messages to all citizens.[30]

Any obligations that require EAS Participants to evaluate, edit or translate EAS messages could undermine the accuracy and timeliness of the information. For these reasons, responsibility for the distribution of multilingual EAS alerts must continue to rest with the emergency managers that create and issue EAS alerts. The Commission endorsed this view only three months ago, stating in the Multilingual EAS Order that alert originators are best positioned to effect multilingual alerting, since broadcast stations are simply passive conduits that automatically relay EAS messages as received, and for the time being, do not have the necessary capabilities to translate or originate alerts in another language.[31] Accordingly, the Commission did not mandate that EAS Participants take any particular steps regarding multilingual EAS, because no such steps may reasonably be required at this time. Instead, the Commission will merely collect information on the status of multilingual EAS in state EAS plans, and specifically clarified that EAS Participants may fulfill this obligation by indicating that no steps to facilitate access to multilingual EAS alerts are warranted, given local circumstances.[32]

NAB submits that, for the sake of consistency, deployment of machine-generated EAS text translation technology should remain a local, voluntary decision by EAS Participants. Technology in this area may be progressing, but at least for the near future may not be reliable enough for EAS Participants to use without concern for accuracy, timeliness, or

---

[30] NAB Comments, EB Docket No. 04-296, at 10-11, (May 28, 2014).
[31] Review of the Emergency Alert System; Independent Spanish Broadcasters Association, the Office of Communication of the United Church of Christ, Inc., and the Minority Media and Telecommunications Council, Petition for Immediate Interim Relief; Randy Gehman Petition for Rulemaking; Order, EB Docket 04-296, FCC 16-32, at 12, (Mar. 30, 2016) (Multilingual EAS Order).
[32] Multilingual EAS Order at 12.

liability for unforeseen problems. Until such time as this technology is fully mature and unfailing, we would encourage the Commission to consider ways to indemnify EAS Participants that choose to deploy new translation technology. This would encourage additional EAS Participants to consider opting for still nascent EAS translation systems.

IV. The Commission's Approach to Enhancing EAS Security is Reasonable Subject to Certain Modifications Designed to Reduce Burden on EAS Participants

A. Broadcasters Take Seriously Their Commitment to EAS Security

The Commission expresses substantial concern about the risks to the security of EAS and the potential impact on the readiness of the EAS system.[33] Unauthorized alerts can also squander government resources, burden EAS Participants, and desensitize the public to actual alerts.[34] The Commission thus proposes new rules intended to more effectively secure EAS, including a requirement that EAS Participants annually certify the performance of certain industry cybersecurity best practices.[35]

The importance of ensuring the reliability of EAS and preserving public confidence in the system cannot be overstated. However, as a preliminary matter, we point out that the Notice cites only a handful of false alerts going back almost a decade in support of Commission action, including the so-called "zombie attack" hoax in 2011, the "Bobby Bones Show" prank in 2014, and a couple of less notorious incidents.[36] In terms of volume and frequency, these occasional hacks, hoaxes and mistakes pale in comparison to the

---

[33] Notice, 31 FCC Rcd at 637.
[34] *Id*.
[35] EAS Participants would be required to certify compliance as part of their new obligation to annually review and update their identifying information in the soon-to-be-launched Emergency Alert System Test Reporting System (ETRS). *Id.*, at 641-642. *See also* Public Notice, *Public Safety and Security Bureau Provides Information on Implementation of EAS Test Reporting System*, PS Docket No. 15-94 (Apr. 18, 2016) (ETRS PN).
[36] Notice, 31 FCC Rcd at 638-639.

hundreds of thousands of weekly, monthly and special EAS tests that occurred during the same period, all without incident, not to mention the infinite number of opportunities for attacks and errors that EAS stakeholders prevented. As the Commission stated after the national EAS test in 2011, the EAS system is fundamentally sound.[37] Attacks on the system and mistaken alerts are few and far between.

NAB does not offer this to minimize the Commission's concerns about EAS security, but merely to highlight the conscientious manner in which EAS Participants and other stakeholders manage the system, and the overwhelming reliability of EAS. Although participation in the EAS system is voluntary, at least on the state and local level,[38] nearly all radio and television stations participate in service of the public interest, and we note, entirely at their own expense. Broadcasters take seriously their commitment to EAS,[39] and should be applauded for their engagement and prodigious efforts to maintain the nation's primary public warning system, rather than rebuked for alleged complacency.[40]

Overall, NAB supports the Commission's general approach to enhancing EAS security. We agree that EAS Participants should have to demonstrate adherence to industry best practices, and we also favor using the industry-generated recommendations approved by CSRIC IV as the basis for those measures.[41] That core elements of EAS security set forth in the CSRIC report and echoed in the Notice are essential: user account management and

---

[37] EAS Test Report at 5.
[38] *See, e.g.*, *Review of the Emergency Alert System, Independent Spanish Broadcasters Association, the Office of Communication of the United Church of Christ, Inc., and the Minority Media and Telecommunications Council, Petition for Immediate Relief*, EB Docket No. 04-296, Second Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 13276, 13283 (2007).
[39] *See, e.g.*, National Public Radio, Inc. Comments, EB Docket No. 04-296, at 2-4, (Nov. 4, 2013).
[40] Notice, 31 FCC Rcd at 640.
[41] CSRIC IV, Working Group 3, Emergency Alert System, *EAS Security Subcommittee Initial Report*, at 11-13, (2014), available at http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-3_Initial-Report_061814.pdf.

password integrity; inspection, software updates and patch management; segmentation and internet-facing firewalls; control over remote access; security training; and the physical security of EAS equipment.[42] NAB also supports the flexibility offered by the Commission to EAS Participants who want to address EAS security through reasonable alternative measures that better suit their particular circumstances.[43] A specific, one-size fit-all mandate is not appropriate in this area.[44] Finally, we support the recommendation made by CSRIC V Working Group (WG) #3 that the Commission ensure that the EAS security best practices are made readily available and EAS participants must know how to find them. CSRIC V WG3 recommended that the best practices be prominently displayed on the Commission's website, possibly in a new Commission document aimed at the station Chief Operator or other individual responsible for EAS operations at each participant facility.[45]

B. The Core Elements of EAS Security Should be Incorporated Within the Commission's Self-Inspection Checklists

Aspects of the Commission's proposed process for compliance with the new EAS security measures may be needlessly heavy-handed. For instance, requiring certification as part of an EAS Participant's duty to update their identification information in the ETRS seems misplaced. The ETRS was created to allow industry and government to "accurately chart what happened in a particular test" of the EAS, and to generate a "Mapbook" of EAS propagation.[46] The ETRS provides a mechanism for EAS Participants to self-identify certain

---

[42] Notice, 31 FCC Rcd at 640.
[43] *Id.*, at 672 (Appendix A, Proposed Rules), 47 C.F.R. §§ 11.44(b)(1)(ii)(A) and (b)(2)(ii)(A).
[44] *Id.*, at 641.
[45] CSRIV V, Working Group 3, *Final Report – EAS Security Best Practices Adoption*, at 10, (2016), available at https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG3_Security_Final_Report_0316.pdf.
[46] ETRS PN at 1.

basic characteristics, such as contact information, facility type, monitoring assignments, and software, and to report on their involvement in a nationwide test.

Researching and completing a certification of compliance with the proposed EAS security measures is a far different matter. Doing so not only entails a thorough technical sweep of a station's facility and process, but also implies almost a virtual guarantee that one's EAS systems are safeguarded against cyber threats. The proposed rules elevate the CSRIC IV EAS security recommendations, which were intended as a voluntary set of guidelines, to regulatory requirements. Thus, as discussed below, many broadcasters will be forced to contract with an IT expert. Including the EAS security certification to the ETRS would fundamentally complicate the nature and purpose of the ETRS system, partly because it raises the specter of Commission enforcement, fines and other remedies for circumstances beyond a station's control. For example, it is quite possible that a broadcast station could perform a thorough analysis that supports an accurate certification of the station's fulfillment of the proposed EAS security measures, only to be hit by a malicious hack that disrupts the station's EAS system. As the Commission is well aware, cybersecurity attacks are on the rise across all industries, including banks, government agencies and other organizations that presumably have the most sophisticated security defenses available.[47]

---

[47] *See, e.g.*, Rajiv Gupta, These Types of Hackers Are Driving Cyber Attacks Now, Fortune, (Mar. 21, 2016), available at http://fortune.com/2016/03/21/cyber-attacks-cybersecurity/, ("Barely two months into 2016, we've already witnessed cybersecurity incidents of unprecedented audacity."); Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattacks, Five Times as Many as Previously Thought*, Washington Post, (Sep. 23, 2015), available at https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/; Mike Lennon, *Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kaspersky Lab*, Security Week, (Feb. 15, 2015), available at http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab.

NAB is concerned that a station would shoulder not only the burden of recovering from an attack, but also be subject to Commission enforcement for a mistaken certification in the ETRS. The Notice lacks any guidance on a broadcaster's potential liability for a false certification, and broadcasters are rightly wary especially given the Commission's recent penchant for imposing tremendous fines on companies for seemingly reasonable rules interpretations, fleeting mistakes, and other problems that can arise despite a station's best efforts.[48] Broadcasters thus question whether the Commission is genuinely interested in granting EAS Participants the flexibility to address EAS security based on their particular circumstances, and if this certification may be another vehicle for enforcement.[49]

The wiser course is to avoid this predicament altogether, and instead treat EAS security like other station technical obligations by incorporating the EAS security measures into the Self-Inspection Checklists that the Commission issues for every segment of broadcast operators: AM, FM, TV, FM Translator, low power FM, and lower power TV, TV translator and TV booster stations.[50] According to the Commission, these checklists "assist broadcast station management in conducting a self-inspection of their station," and "provide

---

[48] *See, e.g.*, Jack Goodman, *$500K Political Ad Fine Cause for Concern*, TVNewsCheck, (Jan. 12, 2016) ("This appears to represent a stunning reversal of longstanding FCC political broadcasting enforcement policies. For at least 25 years, the FCC has taken a light touch to enforcing the political rules. . . The FCC recognized that the political broadcasting rules are ambiguous and stations could in good faith come to different conclusions about how they apply in particular situations. The FCC believed that, if a station made a good faith error, the agency's goals would be better achieved by explaining how the rule should be interpreted in the future, rather than punishing what may have been an innocent mistake. . . . "). Katy Bachman, *Struggling to Make Sense of that WDBJ Fine*, TVNewsCheck, (Apr. 14, 2015) ("The massive $325,000 indecency fine levied on the Schurz Communications CBS affiliate in Roanoke, Va., puzzles an NAB Show panel. 'The infraction was fleeting, it was a fraction of the screen, it was news and most importantly, it was a mistake,' said attorney Dennis Corbett. In addition, the ruling did nothing to clarify the commission's stated goal of going after only "egregious" indecency cases.").

[49] Notice, 31 FCC Rcd at 641.

[50] *See* http://transition.fcc.gov/eb/bc-chklsts/.

an opportunity for the broadcaster to review and correct any deficiencies associated with the operation of a station without an actual on-scene visit by the Commission."[51]

The core elements of EAS security set forth in the Notice are a natural fit for the checklists. They direct stations to affirm that their facilities conform to certain Commission requirements, such as the operational status of their EAS encoder/decoder, the completion of weekly and monthly EAS tests, maximum emission levels, and proper tower lighting, painting and fencing. Similarly, the EAS security elements would direct stations to ensure that EAS equipment is running up-to-date software and hardware, that stations are properly controlling user access to EAS through regularly scheduled password practices, and sufficiently segmenting EAS from the Internet.[52] Adding guidance for EAS security to the checklists would be a logical extension of these technical checks.

Doing so would also have the benefit of expanding the usefulness of the Alternate Broadcast Inspection Program (ABIP), which is a long-successful program that state broadcasting associations (SBAs) administer in partnership with the Commission. Under this program an authorized, experienced ABIP Inspector conducts a thorough inspection of broadcast stations pursuant to the relevant Commission Self-Inspection Checklist. This program enables broadcast stations to undergo a complete assessment by a qualified expert before a visit by Commission staff. As a result, most potential problems are identified by the ABIP Inspector, leading to faster resolutions without taxing the scare resources of either the Commission or the station. Given the success of the ABIP program to identify and correct station technical issues, NAB believes that incorporating the EAS security elements

---

[51] *See, e.g.*, TV Broadcast Station Self-Inspection Checklist, at 5, available at http://transition.fcc.gov/eb/bc-chklsts/EB18TV09_2009.pdf.
[52] Notice, 31 FCC Rcd at 642-645.

into the Self-Inspection Checklists would successfully achieve the Commission's goal to improve EAS security,[53] and through a more reasonable, less-intrusive means than requiring a formal certification from EAS Participants.

C. Annual Certification of EAS Security is Unduly Burdensome

Regardless of the ultimate process for demonstrating EAS security, an annual requirement is too frequent. The Commission underestimates the relevant burden imposed on radio and television stations. A technical sweep of a station's EAS system that is thorough enough for a station to confidently certify compliance on a Commission form will definitely take much longer than the Commission's suggested fifteen minutes.[54] The security elements in the Notice will require running various tests on EAS network and connections, checking firewalls, installing software upgrades, reviewing active user accounts and disabling inactive accounts, double-checking password integrity processes, among other steps. No conscientious broadcaster (or their attorney) would ever file a certification with the Commission without a careful, complete review. Indeed, the National Institute of Standards and Technology (NIST), which produced the Cybersecurity Framework that underlies the Commission's proposed security measures,[55] states that implementing the Framework can take a few weeks to several years, depending on an organization's resources, capabilities, and needs.[56]

---

[53] *Id*., at 641.
[54] *Id*., at 641-642.
[55] The Commission bases its proposed security measures on the best practices recommended in the CSRIC IV Initial EAS Security Report, Notice, 31 FCC Rcd at 641, which is grounded in the NIST Framework for Improving Critical Infrastructure Cybersecurity, (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. *See* CSRIC IV Initial EAS Security Report, at 7.
[56] NIST Cybersecurity Framework Frequently Asked Questions, available at http://www.nist.gov/cyberframework/cybersecurity-framework-faqs-using-the-framework.cfm#long.

The Commission also seems to believe that almost anyone on a broadcaster's staff would be qualified to complete the EAS security certification, comparing this obligation to the preparation of certain filings for the Network Outage Reporting System (NORS).[57] However, NORS filings are typically completed by engineers on staff at large telecom companies and require the input of fairly basic, readily-available information. On the other hand, certifying one's EAS security would require a specialized expert familiar with both EAS and IT security who can sufficiently assess an EAS Participant's network and equipment for cybersecurity risks, that few if any EAS Participants employ such a person in-house, especially smaller and rural radio broadcast stations that have limited resources. Many broadcasters do not even employ a full-time broadcast engineer, instead relying on independent technical consultants that handle such duties for multiple stations in a particular geographic region.[58] While these consultants may possess a range of broadcast engineering skills, cybersecurity IT is likely not one of them. Thus, a substantial number of broadcasters almost certainly will require the expensive assistance of an outside IT consultant to complete a sufficient cybersecurity review, which NAB understands can run into the thousands of dollars.

Rather than an annual obligations, we would strongly urge the Commission to consider a less frequent timetable of perhaps every three years. Such a process would better afford EAS Participants the time and money to conduct a thorough, regularly scheduled assessment of their EAS security. We also support the Commission's suggestion that the EAS security certification requirement should be reviewed within five years with the

[57] Notice, 31 FCC Rcd at 641-642.
[58] CSRIC IV EAS Final Report at 8.

intent to sunset the requirement if EAS Participants are effectively managing the cybersecurity vulnerabilities of EAS.[59] The new compliance process, whether it is annually or less frequent, will inevitably focus the attention of EAS Participants on security to the point where a formal federal certification process is no longer warranted.

D. The Proposed Rules for Collection of Information Regarding EAS Irregularities are Unduly Burdensome and Lack Specificity

The Commission seeks to improve its awareness of EAS anomalies such as false alerts and cable set-top box lockouts that adversely affect the public, stating that more timely notice would help it to assess the nature and impact of such situations, disseminate information to EAS stakeholders, and provide other assistance.[60] Although NAB understands the Commission's interest in collecting such information, we disagree with the proposed process. A requirement that broadcast stations must research, complete and submit an initial report about a false alert within thirty minutes of identification of such a transmission is unreasonable.[61] In many cases, thirty minutes will not be enough time for a station to figure out the nature of the problem at hand. For example, consider a local radio station that carries a syndicated program or brokers part of its schedule, during which a mistaken alert is broadcast, or a station that receives and retransmits an EAS alert as required under the Commission's rules, only to later discover that the alert was mistakenly issued. In such cases, it is reasonable to assume that it will take station personnel much longer than thirty minutes to discern how the false alert started, was mistakenly broadcast, and whether the

[59] Notice, 31 FCC Rcd at 641.
[60] *Id*., at 646-648.
[61] *Id*., at 647. NAB reserves judgment on the proposed obligation that EAS Participants file a final report describing the cause and nature of a false alert within 72 hours. We will rely on the input of EAS Participants who would be more well-versed in the effort needed to prepare such a report.

false alert is due to malicious activity or merely an innocent, unavoidable mistake.[62] The sophistication and variety of cyberattacks is endless and growing, making it increasingly difficult to pinpoint their cause and impact.

A requirement to submit an FCC report within only thirty minutes may compel broadcasters to provide information to the Commission that is incomplete or premature, or even a hasty mischaracterization of the problem. It will also force station staff to halt efforts to resolve the false alert in order to fill out a government form.[63] Instead, NAB would suggest a more reasonable approach that requires an EAS Participant to submit a preliminary initial report about a false alert within three hours after the participant is certain that its broadcast service and EAS equipment are secure. This will allow time for station staff to focus its resources on dealing with the false alert to its conclusion, and provide more accurate information to the Commission.

This is all the more important given the lack of guidance in the Notice about potential penalties for failure to file an initial report about a false alert within the thirty minute period, or for that matter, filing an initial report that turns out to be inaccurate after further investigation. In general, broadcasters and all regulated entities are understandably wary of filing reports to government agencies that characterize problems based on incomplete information. Given recent trends in Commission enforcement, such a report could be subject

---

[62] The Commission's proposed requirement that entities involved in an EAS-related cable set-top box lockout submit an initial report within fifteen minutes of identifying such an incident will be equally difficult to fulfil. *Id*., at 648. NAB submits that it would be impossible for a television broadcaster who "participates in a lockout" to provide any useful information within only fifteen minutes, especially when any such information will presumably lie with the cable operator. Preparing such a report would also distract a broadcaster from working to promptly resolve the problem. NAB can discern no reason the Commission would need this information so quickly.

[63] Marc Solomon, *When Time is of the Essence, Threat Intelligence is Too*, Security Week, (April 24, 2015) ("How quickly defenders can detect and respond to a breach can mean the difference between a nuisance and a nightmare.").

to penalties for lack of candor or misrepresentation, despite a broadcaster's best intentions to file an accurate report. NAB would encourage the Commission to offer some assurance that the Commission merely wants a preliminary picture of an EAS security problem to allow the Commission to help mitigate the situation, and will not refer any such filings (or late or inaccurate filings) to the Enforcement Bureau for enforcement. A reliable, secure EAS system must be a public-private cooperative effort, but unfortunately, the Commission's proposed process for reporting false alerts as it current stands may undermine such cooperation.

Compounding these concerns is the Commission's proposed confidential treatment of initial reports regarding a false alert. The Commission intends to treat the substance of such a report as presumptively confidential, but not the act of filing a false alert report.[64] In support, the Commission equates a false alert report with the proposed EAS security certification that it plans to treat similarly for purposes of confidentiality.[65] This comparison is unpersuasive. The certification serves only to inform the Commission and the public that an EAS Participant has taken steps to address the core elements of EAS security set forth in the Notice.[66] The presence of a certification does not hint at the relative success or failure of those efforts, but merely the fact that some action was taken. A false alert report, on the other hand, unmistakably reveals a problem, regardless of the EAS Participant's level of involvement.

NAB submits that both the act of filing a false report and the substance of such a report should be treated as presumptively confidential. First, it is far too easy to envision

[64] Notice, 31 FCC Rcd at 654.
[65] *Id*.
[66] I*d.*, 31 FCC Rcd at 641.

situations where an EAS Participant must file a false alert report based on incomplete information, only to discover after further investigation that it was faultless, or the problem was mischaracterized, or not a so-called "false alert" at all. For example, virtually all of the broadcasters that relayed the EAS alert in the Bobby Bones incident were completely innocent of any wrongdoing or mistakes, merely fulfilling their function as passive conduits of a properly coded alert.[67] Requiring all such broadcasters to submit a false alert report would be unfair and needlessly embarrassing.

Second, NAB can discern no procedural reason for public disclosure of the act of filing a false alert report, and none is offered by the Commission. Doing so would not facilitate any particular Commission response to a false alert situation, since the Commission would still be privy to the report. There are simply too many uncertainties surrounding the cause, nature and responsibility for false EAS alerts to subject EAS Participants to the ignominy of filing such a report, especially so soon after discovery of a problem and when the EAS Participant may be completely blameless. The better approach is to treat both the act of filing a false alert report and the information on the report as presumptively confidential, and if necessary for some legitimate reason the Commission may provide, allow the filings of such reports to become public at some later point, after an investigation and analysis of the false alert is complete.

E. NAB Supports Addition Of Message Authentication To The EAS.

The Commission seeks comment on the desirability and feasibility of including a unique message ID and/or authenticator ancillary to the EAS Protocol header codes and

[67] Jon Brodkin, *Multi-State Cascade of False Emergency Alerts Nets $1 Million Fine*, ARS Technical, (May 19, 2015).

how to accomplish this in a manner that is technology neutral.[68] It also seeks comment on the advantages and disadvantages of including a digital signature in CAP- and EAS Protocol-formatted EAS messages and on the desirability and feasibility of adopting a Virtual Red Envelope (VRE) solution to alert authentication.[69]

NAB generally supports the addition of message authentication to the EAS. We believe that adding authentication to the EAS protocol and utilizing the digital signature for CAP-based messages would, in theory, improve the reliability of the system. While NAB is agnostic on how best to achieve improved authentication, we offer these observations regarding the legacy EAS protocol. Any additional data that is needed to implement authentication would be carried in the audio portion of a broadcast signal (*i.e.*, using AFSK) in order to be recognized and decoded downstream, thus lengthening the so-called "duck squawk" sound heard by consumers during test and alerts. Even with the VRE solution, we believe that some amount of additional data will be needed in the audio portion of the message. The Commission should consider fully how the sound of this additional data would affect the public. It would be counterproductive if a longer "duck squawk" caused consumers to tune out or change the channel potentially missing the content of the EAS alert.

In addition, given that a very large number of EAS Protocol based alerts that broadcasters receive come from the National Weather Service NOAA Weather Radio System, it is unclear if it also would be updated to include authentication and if not, how would broadcasters and others properly process weather alerts if the commission were to implement authentication technology.

---

[68] Notice, 31 FCC Rcd at 649-651.
[69] *Id*.

Finally, implementation of the authentication technology could require the wholesale replacement of participants EAS Encoded/Decoders. If this is the case, then the proposed one-year compliance deadline is too short. EAS equipment is expensive and broadcasters will require a minimum of two years lead time, and possibly more depending on the cost of the new equipment, to budget and allocate the funds needed to acquire install and test the new gear.

F. Modifications to the Basic Architecture of EAS Should Be Cautiously Considered

The Commission explores a number of wide-ranging, long-term questions about the fundamental structure of the EAS system, such as the benefits of a centralized configuration and EAS management arrangement,[70] and the virtualization of some aspects of EAS equipment and alert dissemination consistent with the ongoing transition of EAS Participants to IP-based platforms.[71] The Commission also seeks comment on the future relationship between the two current pathways for EAS alert distribution, namely, the legacy analog EAS Protocol and the IP-based Common Alerting Protocol (CAP)-formatted IPAWS system.[72]

NAB appreciates the Commission's forethought in launching a dialog about these concepts, and although we respectfully demur at this time to specific comment, we do offer a few general observations for the Commission's consideration. First, as a preliminary matter, the Commission should avoid any steps that could require radio and television stations to purchase new EAS equipment, at least in the short term. It has only been a few of years since EAS Participants were forced to shoulder the costs of new next generation

[70] *Id*., at 657-660.
[71] *Id*., at 661.
[72] *Id*., at 661-662.

equipment capable of receiving and transmitting CAP-formatted EAS messages,[73] which represented a significant portion of many EAS Participants' budgets, particularly smaller and rural radio broadcasters. These broadcasters have many obligations and limited resources, and face a variety of competitive challenges that threaten their economic viability. Frequent reconfigurations of the EAS system that impose additional costs on broadcasters can undercut enthusiasm for participating in EAS. NAB thus encourages the Commission to avoid any measures that would impose any additional burdens on broadcasters.

Second, the Commission should be wary of a singular, centralized point of control of the EAS system. Given the wide variety of EAS encoder/decoders, EAS Participant resources, and a vigorous competitive marketplace for EAS equipment, the matters of who would control such a system is critical. There is also the overriding concern that a single point of control also means a single point of potential failure,[74] and virtualization of parts of the EAS system would also consolidate and connect EAS systems. As malicious hackers continue to outpace industry in terms of sophistication, providing a centralized mechanism for managing the EAS system may be risky. Indeed, one of the main benefits of the existing decentralized organization of EAS is that mistakes and disruptions are inherently hemmed in within a market or region, due to the daisy chain nature of the legacy EAS.

Third, the Commission should avoid changes to the EAS system that overly complicate its use and maintenance for broadcasters, especially by smaller and rural stations that lack the resources and expertise needed to implement an advanced IP system. Many broadcasters prefer a simple EAS box that is easy to install, connect, and maintain or

---

[73] Review of the Emergency Alert System; Independent Spanish Broadcasters Association, the Office of Communication of the United Church of Christ, Inc., and the Minority Media and Telecommunications Council, Petition for Immediate Interim Relief; Randy Gehman Petition for Rulemaking; Fourth Report and Order, EB Docket 04-296, 26 FCC Rcd 13710 (2011).
[74] Notice, 31 FCC Rcd at 657.

upgrade through software patches. Few broadcasters have staff with IP experience, and must engage an expensive outside consultant to handle such duties. A virtualized EAS system may serve only to increase the expense and burden on broadcasters, and undermine the system's current straightforwardness.

Finally, for the time being, NAB supports retaining the dual pathways allowed by the legacy analog EAS system and CAP-formatted IPAWS. The two systems are complementary, and provide important resiliency in the event of a crippling disruption. For example, widespread Internet outages during Hurricane Sandy undercut many broadcasters' ability to monitor CAP-based EAS alerts, while the dissemination of legacy broadcast EAS alerts was not substantially impacted.[75] As of today, the latter is more appropriately considered to be an augmentation of the legacy EAS, rather than a replacement. Going forward, the legacy system will provide an important backup to the IP-based system, and one that could prove critical during emergencies that cause Internet disruptions. We also note that, as the threats to EAS security continue to grow in frequency and sophistication, maintaining the legacy daisy-chain may be even more important, at least until such time that a solely IP-based IPAWS EAS system can be fully safeguarded from disruptions.

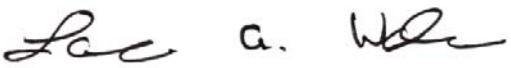
V. Conclusion

For the foregoing reasons, NAB requests that the Commission carefully consider the impact of the proposals set forth in the Notice on radio and television broadcasters. As described above, implementation of many of the proposals may impose costs and burdens on broadcasters that outweigh the intended benefits. Where appropriate, NAB would encourage the Commission to provide EAS Participants with the tools to enhance EAS, and

[75] Joint Comments of Ohio Educational Television Stations, Inc., Monroe Electronics, Inc., and Triveni Digital, Inc., PS Docket No. 15-94, at 7, (May 17, 2016).

allow them the discretion to structure EAS testing and public awareness efforts, and address EAS security consistent with the need and interests of their local communities.

Respectfully submitted,



Rick Kaplan
Larry Walke

NATIONAL ASSOCIATION OF BROADCASTERS
1771 N Street N.W.
Washington, D.C. 20036
(202) 429-5430

Kelly Williams
NAB Technology

June 8, 2016