

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

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

REPLY COMMENTS



AMERICAN CABLE
A S S O C I A T I O N

Matthew M. Polka
President and CEO
American Cable Association
875 Greentree Road
Seven Parkway Center, Suite 755
Pittsburgh, Pennsylvania 15220
(412) 922-8300

Ross J. Lieberman
Senior Vice President of Government Affairs
Mary Lovejoy
Vice President of Government Affairs
American Cable Association
2415 39th Place, NW
Washington, DC 20007
(202) 494-5661

Barbara S. Esbin
Scott C. Friedman
Elizabeth M. Cuttner
Cinnamon Mueller
1875 Eye Street, NW
Suite 700
Washington, DC 20006
(202) 872-6811

Attorneys for American Cable Association

July 8, 2016

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY 1

II. THE RECORD SHOWS THAT THE COMMISSION'S PROPOSAL TO REQUIRE EAS PARTICIPANTS TO CERTIFY TO CSRIC-IV BEST PRACTICES IS BOTH INADVISABLE AND UNNECESSARY 3

 A. Requiring EAS Participants to Certify to CSRIC-IV Best Practices Would Be Overly Burdensome and Disruptive for EAS Participants..... 3

 B. The Isolated Security Incidents Described by the NPRM Do Not Justify Requiring EAS Participants to Certify to CSRIC-IV Practices. 5

III. THE RECORD LACKS ANY BASIS FOR REPLACING FORCE TUNING WITH MANDATORY SELECTIVE OVERRIDES 8

IV. REPORTING REQUIREMENTS FOR FALSE ALERTS OR SET-TOP BOX LOCKOUTS ARE NOT NECESSARY 12

V. COMMENTERS AGREE THAT THE COMMISSION SHOULD NOT EXPAND THE EAS RULES TO REQUIRE CABLE OPERATORS TO PROVIDE EAS ALERTS OVER NEW TECHNOLOGIES OR BEYOND PROGRAMMED CHANNELS 13

VI. CONCLUSION 16

I. INTRODUCTION AND SUMMARY

The American Cable Association (“ACA”) submits these reply comments in response to comments filed concerning the Notice of Proposed Rulemaking (“NPRM”) in the above-captioned docket.¹ While ACA shares the Commission’s goal of a reliable, secure and modern emergency alerting system, in its initial Comments it requested that the Commission refrain from adopting certain proposals put forth in the NPRM that would be particularly burdensome for smaller cable operators and otherwise unnecessary or misdirected. First, ACA asked the Commission to refrain from requiring EAS participants to annually certify compliance with voluntary best practices recommendations for securing EAS equipment made by the Communications Security, Resilience and Interoperability Council IV (“CSRIC-IV”).² Second, ACA recommended that the Commission retain its force tuning and voluntary selective override rules, explaining that the Commission’s policies in this area serve the public interest and remain the best method for ensuring that television viewers receive relevant emergency information in a timely manner.³ Finally, ACA highlighted the lack of need for the Commission’s proposals to (i) adopt false alert and lockout reporting requirements; and (ii) expand the EAS rules beyond traditional MVPD services.⁴

There is overwhelming record support for ACA’s recommendation that the Commission refrain from adopting an annual certification attesting to performance with security measures based on the CSRIC-IV’s proposed best practices. *All* EAS Participants commenting on the

¹ *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System Wireless Emergency Alerts*, Notice of Proposed Rulemaking, PS Docket Nos.15-94 and 15-91 (rel. Jan. 29, 2016) (“NPRM”).

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, Comments of the American Cable Association at 18-23 (filed June 8, 2016) (“ACA Comments”).

³ ACA Comments at 6-17.

⁴ *Id.* at 24-29.

record agree that the Commission's proposal is overly burdensome, unnecessary and would not be effective to secure EAS systems against the incidents described in the NPRM.

The record also supports retention of the Commission's force tuning and voluntary selective override rules. Commenters in favor of replacing force tuning with a selective override mandate put forth *no* evidence to overcome the strong public interest benefits that force tuning provides. Conversely, cable, public interest, and equipment vendor commenters agree that digital technologies, including digital set-top boxes and digital headend technology, have not advanced to a point where selective channel overrides can be readily programmed into most cable operators' equipment. Given the large costs associated with moving from a force tuning to mandatory selective override system and the lack of evidence that force tuning does not serve the public interest, the Commission should retain its current rules.

Similarly, there is little support for reporting requirements covering false alerts and lockouts, events that commenters agree are exceedingly rare. The Commission already requires cable operators to keep a record of each test and activation of the EAS procedures for three years. Adding a reporting requirement on top of this recordkeeping requirement will provide little, if any, additional value.

Finally, commenters uniformly reject the notion of expanding cable operators' EAS obligations, both over new technologies and beyond programmed channels. Cable operators' obligation to broadcast EAS alerts should remain solely over their programmed channels, not other channels on the system such as those used for high-speed data, gaming, or other services, or over emerging video distribution technologies such as TV-Everywhere.

II. THE RECORD SHOWS THAT THE COMMISSION'S PROPOSAL TO REQUIRE EAS PARTICIPANTS TO CERTIFY TO CSRIC-IV BEST PRACTICES IS BOTH INADVISABLE AND UNNECESSARY

The record clearly demonstrates that the Commission's proposal to require EAS Participants to "submit an annual reliability certification form that attests to performance of required security measures with a baseline security posture in four core areas,"⁵ in effect "codify[ing] best practices consistent with CSRIC IV's recommendations,"⁶ is inadvisable, as it would be burdensome and disruptive for EAS Participants, and unnecessary, as there is no evidence of widespread security vulnerabilities among EAS Participants. Furthermore, no commenter objects to providing relief for smaller entities. Even NAB's general support for the Commission's approach to enhancing EAS security is conditioned on the Commission adopting certain burden-reducing modifications.⁷

A. Requiring EAS Participants to Certify to CSRIC-IV Best Practices Would Be Overly Burdensome and Disruptive for EAS Participants.

The record overwhelmingly confirms that the NPRM's description of the proposal as "minimally burdensome"⁸ vastly understates the burdens of submitting an annual certification attesting to certain security measures derived from the CSRIC-IV Working Group 3 EAS

⁵ NPRM, ¶ 111.

⁶ *Id.*, ¶ 109.

⁷ *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, Comments of the National Association of Broadcasters at 13-14 (filed June 8, 2016) ("NAB Comments") ("NAB . . . 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. A specific, one-size fit-all mandate is not appropriate in this area."). One commenter also suggests that the FCC can reduce the burden on EAS Participants by working with FEMA and industry trade groups to work with broadcasters and cable providers on cybersecurity issues for EAS and other broadcast operations. *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, Comments of Adrienne Abbott at 67 (filed June 1, 2016) ("Adrienne Abbott Comments").

⁸ NPRM, ¶ 108.

Security Subcommittee's recommendations.⁹ In fact, *no* commenter puts forth evidence that the proposed certification requirement would not be overly burdensome.¹⁰

Rather, as commenters observe, small EAS Participants in particular may lack the necessary resources and expertise to comply with the proposed certification requirements.¹¹

Because the burdens associated with the proposed certification requirements are so heavy, its adoption by the Commission would have the perverse effect of reducing public safety.

Commenters point out that compliance with the Commission's proposal would stifle EAS

⁹ See *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, Comments of Comcast Corporation at 13-14 (filed June 8, 2016) ("Comcast Comments") ("[T]here would be significant costs and burdens entailed in certifying to each of the specified security practices," and these "would not be limited to the first year of the certification, but would recur annually in light of ongoing network investments, software updates, and personnel changes."); NAB Comments at 18 ("A technical sweep of a [participant's system] that is thorough enough for a [participant] to confidently certify compliance on a Commission form will definitely take much longer than the Commission's suggested fifteen minutes."); *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, Comments of the National Cable & Telecommunications Association at 4-5 (filed June 8, 2016) ("NCTA Comments") ("[I]n light of EAS hardware and software changes, and changes in personnel who run the systems, this process would be an annual undertaking, not simply a year-one exercise. Costs of compliance could exceed millions and millions of dollars per company."). See also Comcast Comments at 13-14 ("As a practical matter, the engineering time, due diligence, and legal review required to prepare a corporate officer to submit a formal declaration would greatly exceed the Commission's estimate.").

¹⁰ One commenter, the New York City Emergency Management Department ("NYCEM"), broadly claims that the "cost estimates . . . are reasonable and would be easily offset by saving the life of at least one human being." *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, Comments of the New York City Emergency Management Department at 1-2 (filed June 8, 2016) ("NYCEM Comments"). NYCEM provides no basis for its claim that the cost estimates are reasonable.

¹¹ Adrienne Abbott Comments at 66; NAB Comments at 19 ("[C]ertifying 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."). Commenters also recommend industry-wide modifications and request that the Commission discuss any potential burdens on the industry. For example, commenters suggest a modified timetable for security certifications – three-year or five-year certification obligations. See NAB Comments at 19; *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, Joint Comments of the Named State Broadcasters Associations at 22-23 (filed June 8, 2016) ("Joint Broadcaster Comments"). Other commenters stress that the Commission must provide further guidance before moving forward with any certification proposal. This includes providing more clarity about which devices and systems are subject to the security requirements, and providing guidance on what would be considered acceptable alternative measures for security concerns. See *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, Comments of AT&T Services, Inc. at 5 (filed June 8, 2016) ("AT&T Comments").

Participants' cybersecurity efforts, rather than advance them, by diverting precious resources away from managing risks and toward compliance.¹² Further, because "industry best practices can and do evolve over time,"¹³ codifying existing CSRIC recommendations could "lock in a checklist of mandatory actions ... thereby *reducing* security as the mandatory actions become obsolete and overtaken by marketplace developments."¹⁴ The record is clear: the proposed requirement that EAS Participants certify to compliance with CSRIC-IV best practices would be unduly burdensome and should not be adopted.

B. The Isolated Security Incidents Described by the NPRM Do Not Justify Requiring EAS Participants to Certify to CSRIC-IV Practices.

The security incidents described by the NPRM do not provide a basis for the Commission to move forward with its certification proposal. ACA agrees with NCTA and other commenters that there is no evidence of systematic, industry-wide failures that would justify such sweeping regulatory intervention,¹⁵ nor is there any reason to believe that the proposed requirements would have prevented the incidents described.

Rather than demonstrating significant vulnerabilities in the nation's EAS infrastructure, the incidents documented in the NPRM "show that there is no systemic weakness in the nation's EAS regime."¹⁶ The highly publicized incidents – the February 2013 "zombie attack" hoax, the

¹² NCTA Comments at 5 ("Contrary to the Commission's broader cybersecurity goals, [the proposed] approach would divert resources away from proactively managing security risks toward checklist compliance."); Comcast Comments at 12 (noting that the proposal "would divert resources from proactive cyber risk management tailored to the specific circumstances of individual EAS Participants"); Joint Broadcaster Comments at 21 ("[T]he draconian measures the Commission proposes in the NPRM are likely to lead to EAS Participants 'shutting down' their EAS activities and doing no more than necessary – airing required tests and Presidential alerts – in order to avoid the penalties incumbent on rule violations for failure to report a breach, report a force-tuning block, certify a software upgrade where Participant resources may not permit such upgrades, or certify security measures such as firewalls in cases where such measures may not be feasible.").

¹³ AT&T Comments at 6.

¹⁴ Comcast Comments at 3.

¹⁵ NCTA Comments at 3; AT&T Comments at 2-3.

¹⁶ AT&T Comments at 2. EAS Participants routinely deliver thousands of EAS alerts to the public annually with limited issues. See NCTA Comments at 3 ("[A]s the Commission has recognized, EAS Participants routinely deliver well over a thousand EAS alerts to the public annually.").

October 2014 “Bobby Bones Show” false alert, and other cited events – are anomalies and do not reflect lingering security vulnerabilities or a general lack of appropriate security practices among EAS Participants.¹⁷

Moreover, the limited incidents described in the NPRM “do not appear to implicate the security practices of non-broadcasters.”¹⁸ ACA emphasized in its Comments that cable operators have significant experience in protecting their networks from malicious attacks.¹⁹ Put simply, there is *no* evidence showing that cable operators’ cybersecurity practices give rise to a need for certification with best practices. Quite the opposite, as cable operators’ cybersecurity practices appear far more developed than other EAS Participants.²⁰

It is also significant that the CSRIC-IV best practices the Commission is considering to codify through the certification requirement would have done little to stop the few incidents identified in the NPRM, which commenters point out were a result of human error and outside the four “core areas” of certification in the proposal.²¹ IPAWS further stresses that the CSRIC-IV Working Group 3 “produced a set of Best Practices related to physical and cyber security of EAS devices” and did *not* “specifically address the security of audio bandpass over-the-air EAS

¹⁷ NAB Comments at 11-12 (“[I]n terms of volume and frequency, these occasional hacks, hoaxes and mistakes [e.g., ‘zombie attack’ hoax of 2011 and the ‘Bobby Bones Show’ prank of 2014] pale in comparison to the 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.”).

¹⁸ AT&T Comments at 3. As AT&T astutely observes, “the lapses identified in the NPRM appear to involve only radio and television broadcast stations.” *Id.*

¹⁹ ACA Comments at 20.

²⁰ NCTA Comments at 6 (“[Cable operators] operate multi-dimensional, sophisticated networks every day and continuously work to monitor and respond to any security vulnerabilities in their infrastructure, including EAS equipment, to ensure a high level of network performance and reliability [and have even] developed higher level security measures than the baseline security practices outlined in the Notice.”).

²¹ Comcast Comments at 10-11 (stating that several of the incidents appear to involve simple human error beyond the scope of any of the four “core areas” identified in the proposed certification); NCTA Comments at 4 (“The [security] incidents cited [by the Commission], some of which involve human error, could occur regardless of how robust an EAS Participant’s security practices are in the four core certification areas in the proposal.”).

transmission.”²² Therefore, according to IPAWS, these best practices *would have had no effect on the Bobby Bones Show incident*.²³ If requiring EAS Participants to certify to CSRIC-IV best practices would have no impact on whether incidents like these reoccur, then there is little to no justification for the Commission’s proposal to require certifications.

Finally, codifying voluntary best practices through a certification requirement is fundamentally inconsistent with the voluntary nature of CSRIC as a government advisory body and would not be a good path to pursue from a policy perspective. Commenters note that the best practices developed in the Final Report by the Working Group were not intended to become regulatory mandates.²⁴ Moreover, to the extent there are EAS security vulnerabilities, the proposed certification requirement would depart from the Commission’s prior efforts to promote effective cybersecurity risk management across the communications sector through stakeholder efforts focused on voluntary implementation.²⁵

In short, the record soundly refutes the Commission’s justification of its certification proposal based on these isolated incidents.

²² *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, Comments of the Federal Emergency Management Agency Integrated Public Alert and Warning System Program Management Office at 4 (filed June 8, 2016).

²³ *Id.* (emphasis added). See also *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, Comments of Sage Alerting Systems, Inc. (filed June 8, 2016) (“Sage Comments”) (“We also note that, by itself, a digital signature would not be sufficient to thwart a new Bobby Bones incident. Had the gag replayed an alert with a digital signature, the signature could still be valid. Strict adherence to the valid time of an EAS message is critical to avoiding replay errors, even if the alert does contain a digital signature.”).

²⁴ NCTA Comments at 4.

²⁵ Comcast Comments at 12.

III. THE RECORD LACKS ANY BASIS FOR REPLACING FORCE TUNING WITH MANDATORY SELECTIVE OVERRIDES

In response to requests from the broadcast industry, the NPRM seeks comment on whether the Commission should no longer allow cable operators to force tune and, instead, be required to “refrain from interrupting local broadcast programming where the broadcast provider is participating in the EAS system.”²⁶ The few commenters in favor of replacing force tuning put forth *no* evidence to overcome the strong showing in the record of the public interest benefits that force tuning provides. Accordingly, the Commission should preserve its current approach, which utilizes force tuning, with the option for voluntary selection override arrangements between cable operators and broadcasters only where technically feasible and appropriate.²⁷

Force tuning ensures that EAS Participants who do send out state and local alerts, which ACA members serving rural and small market areas mostly do, reach members of their local communities with pertinent and timely information. Public safety commenters acknowledge that it is of the utmost importance that emergency information is broadcast and displayed to the general public as widely as possible.²⁸ Were the Commission to eliminate the force tuning requirement and instead require the selective override of broadcast stations, some members of the public could lose access to important state and local EAS alerts. As the

²⁶ NPRM, ¶¶ 80, 84.

²⁷ The Commission itself has concluded on multiple occasions that allowing cable operators the flexibility to deliver EAS alerts by force tuning set-top boxes to an EAS dedicated channel remains, in most instances, the best way to ensure that viewers receive emergency information that is important to them. See ACA Comments at 6-13. See also *Amendment of Part 73, Subpart G, of the Commission’s Rules Regarding the Emergency Broadcast System*, Report and Order and Further Notice of Proposed Rulemaking, 10 FCC Rcd 1786 (1994); *Amendment of Part 73, Subpart G, of the Commission’s Rules Regarding the Emergency Broadcast System*, Second Report and Order, 12 FCC Rcd 15503 (1997); *Amendment of Part 73, Subpart G, of the Commission’s Rules Regarding the Emergency Broadcast System*, Third Report and Order, 14 FCC Rcd 1273 (1998) (“Third Report and Order”); *Amendment of Part 11 of the Commission’s Rules Regarding the Emergency Alert System*, Report and Order, 17 FCC Rcd 4055 (2002). Other commenters agree. See NCTA Comments at 13 (“The Commission has consistently (and repeatedly) concluded that whether selective override is beneficial to the public depends on local facts and circumstances, and that in some cases it could be detrimental to a cable operator’s ability to alert its subscribers to local emergencies.”).

²⁸ NYCEM Comments at 5-6.

Commission has recognized, “because broadcast stations often serve a wide coverage area crossing hundreds of communities, they may not cover local emergencies that affect only a single community.”²⁹ Additionally, because the geography of some designated market areas does not always align with state boundaries, viewers may not receive their own state EAS alerts if their “in-market” broadcast station is located in a neighboring state.³⁰ Requiring selective override could prevent viewers in these areas from receiving EAS messages, even if their local broadcast station participates in their state and local EAS programs.

Commenters have offered *no* evidence to rebut the fact that requiring selective overrides will deprive some members of the public from receiving emergency alerts.³¹ To the contrary, NAB curiously claims that local “stations receive and broadcast the exact same EAS message content that the cable operator provides on its designated [EAS] channel,”³² even though state and local area plans under the FCC’s EAS rules do *not* correlate with DMA boundaries.³³

Commenter arguments that focus on force tune disruptions similarly fail to rebut the substantial public interest benefits that force tuning provides. The New York City Emergency Management Department (“NYCEM”) lists “widespread disruptions” from past force tuning

²⁹ Third Report and Order, ¶ 13.

³⁰ See *In-State Broadcast Programming: Report to Congress Pursuant to Section 304 of the Satellite Television Extension and Localism Act of 2010*, Report, 26 FCC Rcd 11919, at Appendix F (2011) (case study discussing 35 counties in 13 DMAs with little or no access to in-state broadcast stations via satellite service). See also *Amendment to the Commission’s Rules Concerning Market Modification, Implementation of Section 102 of the STELA Reauthorization Act of 2014*, Report and Order, MB Docket No. 15-71, ¶ 3, n.5 (rel. Sept. 2, 2015) (“The inability of satellite subscribers located in ‘orphan counties’ to access in-state programming has been the subject of some congressional interest.”).

³¹ See also NCTA Comments at 14 (“[T]here is no technical or policy basis for the Commission to reexamine the [force tuning] rules yet again.”); *Amendment of Part 11 of the Commission’s Rules Regarding the Emergency Alert System*, PS Docket No. 15-94, Reply Comments of Frank W. Bell at 9 (filed June 14, 2016) (“Bell Reply Comments”) (“The NAB opposition to force-tuning TV channels covering the area with EAS alerts is something that has been discussed for too long.”).

³² NAB Comments at 10.

³³ See 47 C.F.R. § 11.21(b) (“A Local Area is a geographical area of contiguous communities or counties that may include more than one state.”). ACA reviewed a number of state EAS plans and can confirm that, in many instances, local area plans will cross DMA boundaries or the DMA will be divided into multiple local plans.

experiences as a “compelling reason” for the FCC to permit alternative forms of EAS delivery,³⁴ while another commenter claims that required monthly tests, when broadcast separately by a broadcast station and cable operator, have proven to be confusing to members of the public.³⁵ ACA pointed out in its Comments that such instances appear to be rare, and in no way offset the public interest benefits of ensuring that emergency alerts are disseminated as widely as possible.³⁶ Further, the Commission’s rules also do not prohibit selective override, and “where cable operators have flexibility under their franchise agreements, where they have newer, upgraded equipment in place, and where it benefits their customers, they have worked with broadcasters to omit their stations from all-channel EAS overrides.”³⁷

Finally, there is general agreement among cable, public interest, and equipment vendor commenters that digital technologies, including digital set-top boxes and digital headend technology, have not advanced to a point where selective channel overrides can be readily programmed into most cable operators’ equipment, especially in the case of smaller providers. ACA explained in its Comments that while selective override technology exists, most set-top box software deployed by cable operators does not support selective overrides and, therefore, a selective override requirement would require cable operators to purchase new software and, depending on the operator, possibly hardware as well.³⁸ Moreover, mandating selective overrides would require cable operators to program their systems to provide EAS alerts only on

³⁴ NYCEM Comments at 6-7.

³⁵ *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, Letter from Ed Brouder, Executive Director, SECC Chair, New Hampshire Association of Broadcasters, to Marlene H. Dortch, Secretary, FCC, at 9-10 (filed June 1, 2016) (“Brouder Letter”).

³⁶ ACA Comments at 16 (“Given the sheer number of required EAS tests and local EAS alerts that occur each year, [the lack of glitches] is not surprising – the EAS system and EAS equipment are thoroughly tested on a regular basis. While the NPRM cites ‘multiple informal complaints from consumers claiming they were unable to change channels after being force tuned due to an EAS Alert,’ ACA is not aware of any formal Commission action taken in response to these complaints.”).

³⁷ NCTA Comments at 13.

³⁸ ACA Comments at 13-15.

non-broadcast channels, which is significantly more complicated than sending a single alert across the entire programming lineup, especially for smaller operators with limited financial and administrative resources.

Commenters industry-wide share ACA's concern that mandatory selective overrides would be burdensome. Trilithic, an EAS equipment manufacturer, explains that "force tuning is often the most cost effective and efficient method to present EAS messages on all channels with [a cable operator's] system."³⁹ Non-cable commenters even recognize that small and medium-sized cable operators could be severely hurt were the Commission to mandate selective overrides. For example, one commenter recognizes the adverse economic impact of such a requirement on cable operators offering service in small, hard-to-serve communities that are unreachable by broadcast signals.⁴⁰ In a similar vein, NCTA describes how, consistent with Commission precedent, cable operators have developed systems based on force tuning and that revising the Commission's rules to abandon force tuning is *not* feasible, such that any plausible public interest benefits would be outweighed by the significant costs and burdens imposed on cable systems.⁴¹ This is due to the "massive overhaul of cable operators' video networks [that would be necessary] – among other things, EAS software and hardware components, including EAS encoders/decoders, set-top control equipment, and set-top boxes would all need to be replaced or reprogrammed."⁴² Such a dramatic change would inevitability

³⁹ *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, Comments of Trilithic, Inc. at 5 (filed June 8, 2016).

⁴⁰ Adrienne Abbott Comments at 57 ("There are several smaller cable providers in Nevada who do not have the financial resources to add new equipment. Several local cable companies are community operated, including the cable system in Virginia City, Nevada. Comstock Cable TV has approximately 30 subscribers and operates as a non-profit business. The area is mountainous, surrounded by steep, rocky terrain unsuitable for receiving broadcast signals and without the southern exposure needed for satellite service. Any new requirements for equipment would place a severe financial strain on the company and put the cost of service out of reach for most of the subscribers.").

⁴¹ NCTA Comments at 11.

⁴² *Id.* at 12.

“result in higher costs being passed along to consumers, and would not be in the public interest.”⁴³

Accordingly, given the lack of evidence that force tuning does not serve the public interest and the large costs associated with moving from a force tuning to selective override system, the Commission should retain its current rules.

IV. REPORTING REQUIREMENTS FOR FALSE ALERTS OR SET-TOP BOX LOCKOUTS ARE NOT NECESSARY

The record overwhelmingly demonstrates that false alerts and lockouts are rare and that reporting requirements are unnecessary. NAB correctly notes that even the Commission has observed that the EAS system is fundamentally sound, and that attacks on the system and false alerts are rare.⁴⁴ AT&T, as well, highlights the fact that lockouts are “infrequent.”⁴⁵

Moreover, reporting on false EAS transmissions and lockouts would be difficult and expensive for cable operators because “operators have no way to determine that an EAS transmission is false using current equipment, unless someone is actually watching the feed for EAS alerts, which would be expensive and time-consuming.”⁴⁶ Cable operators would also be forced to screen EAS alerts to watch for potentially false alerts, and verifying EAS alerts straightaway could also delay delivery of an alert to the public, which, in turn, could pose a significant public safety hazard. In the case of an actual false alert, reporting would also take valuable time away from fixing the underlying issue.⁴⁷ To this end, the proposed reporting timelines are completely unrealistic.⁴⁸

⁴³ *Id.*

⁴⁴ NAB Comments at 13.

⁴⁵ AT&T Comments at 7.

⁴⁶ NCTA Comments at 8.

⁴⁷ AT&T Comments at 7 (“[EAS Participants] should spend those first few minutes trying to resolve the lockout, not hastily compiling and submitting some report.”).

⁴⁸ Joint Broadcaster Comments at 22 (“[T]he proposed 15 minute/30 minute timelines for reporting certain breaches are completely unrealistic.”); NAB Comments at 20 (“A requirement that [an EAS Participant] research, complete and submit an initial report about a false alert within thirty minutes of identification of

Only one commenter – NYCEM – filed in support of the Commission’s proposal, arguing that a reporting requirement would allow the agency to be aware of the problem and ensure that corrective actions are taken to prevent similar future situations.⁴⁹ To the extent that an EAS incident, such as a false alert, must be investigated, the Commission can request that the cable operator turn over its EAS logs, in which the cable operator must keep a record of each test and activation of the EAS procedures for three years.⁵⁰ Adding a reporting requirement on top of this recordkeeping requirement will provide little, if any, additional value.

V. COMMENTERS AGREE THAT THE COMMISSION SHOULD NOT EXPAND THE EAS RULES TO REQUIRE CABLE OPERATORS TO PROVIDE EAS ALERTS OVER NEW TECHNOLOGIES OR BEYOND PROGRAMMED CHANNELS

In the NPRM, the Commission seeks comment on expanding EAS alerts to include new and emerging technologies and services.⁵¹ In both instances, commenters overwhelmingly reject the notion of expanding cable operators’ EAS obligations.

NCTA agrees with ACA that cable operators should not be required to support EAS alerts on new technologies. Such a requirement would “create an uneven playing field in the

such a transmission is unreasonable. In many cases, thirty minutes will not be enough time for a station to figure out the nature of the problem at hand.”); Brouder Letter at 11 (““Requiring stations to report false alerts may prove a difficult exercise. There is a presumption that all stations will immediately know a false alert has occurred, which isn’t necessarily the case. Unattended stations may well have a contract engineer who checks EAS logs on a regular basis but not daily. It could be several days before an anomaly is noticed if the station is normally unmanned. I have found it exceedingly difficult to track backwards to figure out how a given station handled a particular test or activation if no one was in the building in the first place.”); AT&T Comments at 8 (“In order to submit a final report detailing the root cause of the lockout, the number of affected customers, and ‘mitigation steps taken,’ AT&T proposes the Commission provide filers up to 60 days. As the Commission explains, lockouts are unusual events. This means EAS Participants and their personnel have little or no experience with them, and performing what is likely to be a novel analysis for these employees will require more than a few days. This analysis might (or, perhaps, is likely to) implicate some unaffiliated entity, which could further delay the identification of the root cause of the lockout.”).

⁴⁹ NYCEM Comments at 10.

⁵⁰ See 47 C.F.R. §§ 76.1700(c)(3); 76.1611.

⁵¹ NPRM, ¶¶ 85-86; 88-89. This includes “initiat[ing] a conversation” on the delivery of EAS alerts over new technologies, including over-the-top type delivery, and whether cable operators should be required to provide EAS alerts beyond programmed channels to include “channels used for the transmission of data such as interactive games,” “channels used for the transmission of data services such as Internet,” or “channels used for the transmission of data services such as Internet access.” *Id.*, ¶¶ 85-86.

market for OTT video services, harming competition and deterring innovation by subjecting certain providers to regulatory burdens that would not apply to their competitors.”⁵² Additionally, “[w]hether IP cable service is delivered via a set-top box or an app, the service delivers EAS messages consistent with the Commission’s Part 11 rules. In contrast, video that is delivered in IP on the public Internet does not support EAS.”⁵³

Commenters, including public safety commenters, also concur with ACA that customers do not expect to receive EAS alerts over new and emerging technologies.⁵⁴ EAS alerts are often highly localized. Receiving local EAS alerts when using over-the-top video services, often accessible nationwide so long as the consumer authenticates, would likely confuse consumers, especially since they have no expectation of receiving them in an “online environment.”⁵⁵ To the extent that consumers want to receive EAS alerts on new technologies, “there are numerous resources available today to meet that need in the absence of government mandates.”⁵⁶

Nor is there any basis for the Commission to require cable operators to provide EAS alerts beyond programmed channels. Rather, the record supports continuation of the Commission’s practice of distinguishing “programmed” channels subject to EAS requirements from other features or services provided by EAS Participants.

First, commenters agree with ACA that the Commission does not have the statutory authority to expand its EAS rules in the manner contemplated. By the Commission’s own

⁵² NCTA Comments at 20.

⁵³ *Id.* at 17.

⁵⁴ See Adrienne Abbott Comments at 60-61 (“Consumers in Nevada expect to receive EAS messages which apply to them directly, not to the people on the other side of town or the next valley over the hill.”); NYCEM Comments at 8 (expressing concern “that a viewer could be watching a broadcast from their mobile device that would be relevant to them at their place of residence or employment but not necessarily relevant to them at their present location.”).

⁵⁵ Comcast Comments at 2-3; *see also* NCTA Comments at 19 (“Consumers have no expectation that they will receive EAS alerts on OTT video services watched on mobile devices outside the home. To be sure, consumers expect EAS messages (which generally convey information about local emergencies) when watching television programming on broadcast or MVPD platforms in the home.”).

⁵⁶ Comcast Comments at 10.

definition, the statutory grant of authority to impose EAS obligations on cable operators is based on emergency information being provided to viewers of “video programming on cable systems.”⁵⁷ Expanding the EAS requirements to all “channels that are made available for consumer use” would, arguably, expand the scope of EAS requirements to non-cable services.⁵⁸

Second, beyond commenters’ legal arguments, NCTA agrees with ACA that there currently is no means by which cable operators can provide EAS alerts across “all” channels, emphasizing that expanding EAS alerts to non-programmed channels would have “significant technical implications for cable EAS infrastructure.”⁵⁹

⁵⁷ NCTA Comments at 15. See *also* Comcast Comments at 6 (agreeing with ACA and NCTA that the current approach should be maintained since it follows “unambiguous statutory language, tracks consumer expectations regarding the receipt of EAS alerts, and clearly delineates how EAS messages are to be delivered over cable systems.”).

⁵⁸ Comcast Comments at 6.

⁵⁹ NCTA Comments at 16.

VI. CONCLUSION

ACA and its members share the Commission's desire to ensure an effective, secure and modern emergency alerting system that delivers relevant alerting messages in a timely fashion. The record in this proceeding conclusively demonstrates, however, that none of the proposals concerning certification with CSRIC best practices, requiring selective overrides, reporting requirements for false alerts or lockouts, or expansion of the EAS rules to new technologies or beyond programmed channels are warranted or should be adopted as proposed.

Respectfully submitted,

AMERICAN CABLE ASSOCIATION



By: _____

Matthew M. Polka
President and CEO
American Cable Association
875 Greentree Road
Seven Parkway Center, Suite 755
Pittsburgh, Pennsylvania 15220
(412) 922-8300

Ross J. Lieberman
Senior Vice President of Government Affairs
Mary Lovejoy
Vice President of Government Affairs
American Cable Association
2415 39th Place, NW
Washington, DC 20007
(202) 494-5661

Barbara S. Esbin
Scott C. Friedman
Elizabeth M. Cuttner
Cinnamon Mueller
1875 Eye Street, NW
Suite 700
Washington, DC 20006
(202) 872-6811

Attorneys for American Cable Association

July 8, 2016