

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

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

**COMMENTS OF THE
NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION**

William A. Check, Ph.D.
Senior Vice President, Science & Technology
Chief Technology Officer

Andy Scott
Vice President, Engineering
Science & Technology

June 8, 2016

Rick Chessen
Loretta Polk
Stephanie L. Poday
National Cable & Telecommunications
Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY1

I. THE COMMISSION SHOULD DECLINE TO ADOPT THE CERTIFICATION PROGRAM AND OTHER PROPOSALS.2

 A. The Proposed Certification Program is Unnecessary and Overly Prescriptive.2

 B. Given the Infrequency of False Alerts and Lockouts, the Commission Should Not Impose a Reporting Regime.8

 C. Instituting New Alert Authentication and Alert Validation Requirements Is Not Technically Feasible Today and Would Be Costly to Implement.....9

II. THE COMMISSION SHOULD STREAMLINE THE PROPOSALS IT CONSIDERS IN DEVELOPMENT OF ANY VOLUNTARY INDUSTRY ROADMAP.....10

 A. New EAS Proposals That Would Fundamentally Alter Existing Cable EAS Infrastructure Are Not Viable.11

 B. The Commission Should Not Explore Disparate Regulatory Treatment of EAS Participants Offering OTT Services.16

 C. New Translation or Accessibility Requirements Are Unnecessary.....20

III. THE COMMISSION SHOULD CONVENE A MULTI-STAKEHOLDER INITIATIVE TO CONSIDER THE MIGRATION TO PRIMARY IP DELIVERY OF EAS ALERTS.....21

CONCLUSION.....23

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

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

**COMMENTS OF THE
NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION**

The National Cable & Telecommunications Association¹ hereby submits its comments on the *Notice of Proposed Rulemaking (“Notice”)* in the above-captioned proceedings.²

INTRODUCTION AND SUMMARY

Cable operators are proud of the considerable investments they have made over many years to provide important Emergency Alert System (“EAS”) messages to their customers. Our industry’s commitment has resulted in a robust and well-functioning EAS system, where operators deliver hundreds and hundreds of messages annually to cable customers in all kinds of emergency situations.

The cable industry is open to modernization of EAS given advancements in digital and Internet Protocol (IP) technology to make alerting more valuable to the public and commends the Commission for initiating the dialogue on ways to enhance state and local community alerting. However, modernization and next generation EAS efforts should be done through thoughtful

¹ NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 percent of the nation’s cable television households and more than 200 cable program networks. The cable industry is the nation’s largest provider of broadband service after investing over \$245 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to approximately 30 million customers.

² See *In re Amendment of Part 11 of the Commission’s Rules Regarding the Emergency Alert System, Wireless Emergency Alerts*, Notice of Proposed Rulemaking, 31 FCC Rcd 594 (2016) (“*Notice*”).

study and analysis with EAS participants working together with government partners, not through ad hoc rule changes. Until such comprehensive, future-oriented analysis is done, the current EAS regime should be maintained – not dramatically reconstituted.

In particular, the Commission should decline to adopt proposals that would (1) require a new EAS certification program; (2) impose any new requirements related to authenticating and validating alerts; (3) fundamentally alter how cable operators deliver EAS alerts; and (4) apply EAS obligations to video services provided by EAS Participants over the Internet. These proposals raise significant concerns for cable operators because, among other things, they are unwarranted by the facts, technically infeasible, and costly to implement.

The cable industry supports continued discussion about improving EAS but a more constructive way to proceed is for the Commission to convene a multi-stakeholder initiative to examine how to best leverage the benefits of Internet Protocol and other technological advancements to develop a new EAS alert system that would utilize IP in the first instance in delivering alerts to EAS Participants, while maintaining the legacy daisy chain as a back-up delivery method.

I. THE COMMISSION SHOULD DECLINE TO ADOPT THE CERTIFICATION PROGRAM AND OTHER PROPOSALS.

A. The Proposed Certification Program is Unnecessary and Overly Prescriptive.

The *Notice* proposes a comprehensive annual certification program to codify EAS security best practices consistent with the recommendations developed by the Communications Security Reliability and Interoperability Council (CSRIC) in its voluntary advisory role. Under the proposal, EAS Participants would be required to submit “an annual reliability certification form that attests to performance of required security measures with a baseline security posture in four core areas,” patch management, account management, segmentation and validation of

digital signatures on Common Alert Protocol (CAP) messages.³ If a company does not conform to the elements specified in the rules, it would be required to explain and certify whether it has taken “alternative measures or remediation to meet or exceed the security provided by” the particular mandated security measure.⁴

As a factual matter, it is not clear that such a certification would prevent reoccurrence of security incidents identified in the *Notice*. As a policy matter, a mandatory certification of compliance with certain practices for EAS should not be grounded in *voluntary* best practices developed under the agency’s CSRIC Advisory Committee. The Commission should reevaluate the certification concept for several reasons.

First, there is no evidence of systematic, industry-wide failures that would warrant such sweeping regulatory intervention. The Commission bases its proposal on certain EAS security incidents that occurred over the past nine years, which it believes demonstrate that “there are significant vulnerabilities in the nation’s EAS infrastructure that must be addressed comprehensively.”⁵ But, as the Commission has recognized, EAS Participants routinely deliver well over a thousand EAS alerts to the public annually.⁶ The *Notice* cites two incidents, the hackers who executed the 2013 “zombie attack” hoax and the 2014 “Bobby Bones Show” false alert, as well as several other accidental EAS activations, but none of these incidents reflect a

³ *Notice* ¶ 111.

⁴ *Id.* Appendix A, § 11.44 (b)(1)(ii).

⁵ *Id.* ¶ 97.

⁶ *See In re Review of the Emergency Alert System; Indep. Spanish Broad. Ass’n, the Office of Communication of the United Church of Christ, and the Minority Media & Telecom. Council, Petition for Immediate Relief, Randy Gehman Petition for Rulemaking, Fifth Report & Order, 27 FCC Rcd 642 ¶ 6 (2012)* (stating that “EAS Participants deliver well over a thousand alerts issued by state and local governments and the NWS [National Weather Service] annually, the vast majority of which are weather related alerts”). The NWS reports that it generates “about 90% of EAS activations, primarily for short-duration weather warnings and watches.” Nat’l Oceanic & Atmospheric Admin., *EAS Factsheet*, Apr. 2016, available at http://www.nws.noaa.gov/nwr/resources/EAS_factsheet.pdf.

widespread EAS security breakdown among EAS Participants. The incidents cited, 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. Taken together, these inadvertent EAS transmissions do not reveal an unacceptably high risk of unauthorized EAS alerting to warrant new rules. Moreover, where EAS security incidents occasionally occur, the Commission readily exercises its enforcement authority to impose significant fines and take other action against the EAS Participant to address such incidents.⁷

Second, the *Notice* contends that the proposal seeks to “codify best practices consistent with” CSRIC IV, Working Group 3, recommendations,⁸ but this approach is fundamentally inconsistent with the *voluntary* nature of CSRIC as a government advisory body. The best practices developed in the Final Report by the working group were not intended to become regulatory mandates.⁹ This departure from the recommended approach by participants in CSRIC is particularly notable given the Commission’s focus on a “new paradigm” of industry-driven proactive solutions that is distinct from reactive compliance with prescriptive rules and a cybersecurity to-do list that cannot keep pace with dynamic and innovative communications systems.¹⁰ Moreover, while the *Notice* asserts that the proposed certification would provide EAS Participants “ample flexibility” in implementing core security mechanisms and that it is “intended to complement, rather than replace, the Commission’s current support for voluntary

⁷ See, e.g., *In re iHeartCommunications*, Order, 30 FCC Rcd 4442 (2015) (enforcement investigation resulting in \$1 million fine assessed for misuse of EAS tones on a distributor of syndicated radio programming).

⁸ *Notice* ¶ 109.

⁹ See CSRIC IV Working Group 3, EAS Security Best Practices, Final Report (2015), available at https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG3-EAS_SECURITY_FINAL_011316.pdf (“*CSRIC IV WG3 Final Report*”).

¹⁰ See e.g., Remarks of Chairman Thomas Wheeler, American Enterprise Institute, June 12, 2014 (“[W]e cannot hope to keep up [with cyber threat technology obsolescence] if we adopt a prescriptive regulatory approach.”), available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-27591A1.pdf.

implementation of best practices developed through cooperation with industry and advisory bodies,”¹¹ the fact of the matter is that the certification regime would constitute a regulatory mandate that would place the burden on EAS Participants to explain why they believe their chosen security practices are “reasonably sufficient”¹² and to face potential penalties if the Commission disagrees with their chosen approach. Such government intrusion into EAS Participants’ individual risk management decisions is simply not warranted by the facts and circumstances presented in the *Notice*.

Third, the Commission significantly underestimates the cost and burden of certifying compliance with each security measure or practice for thousands of facilities nationwide. The Commission rightfully seeks comment on the relative costs and benefits of its certification program but suggests at the outset that this mandate would be “minimally burdensome” or involve “no additional cost.”¹³ It estimates, for example, that the certification should add “an average of fifteen minutes to the annual update of the “identifying information” section in the ETRS resulting in an increased cost to industry of approximately \$549,360 per year.”¹⁴ It further assumes that if legal and management review is required, it would only be required in the first year and would amount to no more than an average of one hour per company for an additional \$2,179,440 the first year.¹⁵

These estimates understate the costs of compliance. Corporate regulatory compliance programs involve a systematic process of technical, engineering, and operations due diligence followed by legal and management review and rigorous testing before a corporate officer

¹¹ *Notice* ¶ 109.

¹² *See Notice*, Appendix A § 11.44(b)(ii).

¹³ *Notice* ¶ 111, 117.

¹⁴ *Id.* ¶ 111.

¹⁵ *Id.*

certifies a submission to the government that is subject to penalty for inaccuracies and incurs the cost of a compliance audit. In 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. Contrary to the Commission's broader cybersecurity goals, this approach would divert resources away from proactively managing security risks toward checklist compliance.

Finally, operators already have strong market-based incentives to ensure the safety and security of their EAS systems, as with every other function in their business and network operations. The Commission is well aware that cable companies 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.¹⁶ This is a fundamental component of their enterprise risk management strategy. As part of this effort, NCTA's members take seriously their responsibility to ensure that their customers receive timely and accurate emergency information and EAS alerts. Many have developed higher level security measures than the baseline security practices outlined in the *Notice*.

We urge the Commission, therefore, to resist imposing regulatory mandates for EAS security that will only constrain the reasonable business judgment and risk management activities of companies that operate these networks day-to-day. The Commission should continue to rely on and promote the important best practices and voluntary standardization efforts for EAS, rather than impose a new government-sponsored certification program. The public-private partnership

¹⁶ See, e.g., NCTA Comments, in response to FCC, Public Notice, *FCC'S Public Safety & Homeland Security Bureau Requests Comment on Implementation of CSRIC III Best Practices*, DA 14-1066, 29 FCC Rcd 9217 (filed Sept. 26, 2014).

efforts to address EAS vulnerabilities should be continued, perhaps with particular emphasis on improving personnel training, through various forms of outreach to companies.¹⁷

If the Commission goes forward with a certification program of some type despite the defects in the proposal, it must ensure the confidentiality of all information provided by EAS Participants. The *Notice* tentatively concludes and the proposed rules reflect that “the act of filing (or not filing) an annual certification” and “responses on the face” of certification forms “should not be treated as presumptively confidential.”¹⁸ Only data reported on the certification and information that “consists of descriptions and documentation of alternative measures to mitigate the risks of nonconformance with certification elements” are presumed confidential.¹⁹ To avoid any confusion resulting in disclosure of sensitive critical infrastructure information, *all* data supplied by an EAS Participant, whether simply on the face of a form or in more descriptive detail, should be treated as confidential and protected from disclosure.

The *Notice* also asks, if it adopts presumptively confidential certification and reporting requirements, whether the Commission should share information from thousands of EAS Participants with other federal agencies, state entities – and suggests even non-governmental entities might be authorized to receive the information. While the Commission may intend to share such information to strengthen the nation’s public alert and warning systems, this raises a far greater risk of exposing critical cybersecurity information to those who wish to bring harm to communications systems or to competitors who may seek economic advantage. We oppose sharing EAS security information outside of the Commission given these substantial risks.

¹⁷ See *CSRIC IV WG3 Final Report*.

¹⁸ *Notice* Appendix A, § 11.44 (c)(1)(i); *id.* ¶ 148.

¹⁹ *Id.* Appendix A, § 11.44 (c)(1)(ii).

However, if some type of information sharing is adopted, NCTA believes that it should only be done under the auspices of the U.S. Department of Homeland Security's comprehensive Protected Critical Infrastructure Information (PCII) program or a legally sustainable equivalent. The PCII Program provides, among other things, a mechanism for critical infrastructure owners and operators to share information with DHS and other qualifying entities, while ensuring that such information remains protected and exempt from federal and state disclosure laws and use for regulatory purposes.²⁰ In the context of CSRIC, the Commission endorsed sharing cybersecurity information provided it is treated as PCII. Such action would be necessary given the inadequacy of the limited confidentiality provisions in the certification proposal.

B. Given the Infrequency of False Alerts and Lockouts, the Commission Should Not Impose a Reporting Regime.

The *Notice* proposes to require EAS Participants to report on instances of false EAS transmissions and lockouts that adversely affect the public. This would be difficult and expensive for cable operators to do. In our member companies' experience, false alerts and lockouts rarely happen. Cable operators disseminate EAS alerts on an automated basis, often from facilities that are not staffed 24 hours per day. Moreover, existing log information does not provide enough detail to know whether a particular EAS message would trigger a reporting obligation under the proposal in the *Notice*. Accordingly, 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. Even then, without actual knowledge of the emergency at issue, it would be difficult to determine if the alert was false. Accordingly, any proposed technology solution would require extensive work and cost to determine the feasibility of authenticating every EAS message. To the extent false alerts and

²⁰ See Procedures for Handling Critical Infrastructure Information; Final Rule, 6 C.F.R. § 29.3 (2006).

lockouts occur, reporting would be an unnecessary distraction from addressing their root cause. Any requirement to detect and report on lockouts would be unduly burdensome without a clear connection between the Commission's collection of such information and actual improvements in lockout prevention or response.

C. Instituting New Alert Authentication and Alert Validation Requirements Is Not Technically Feasible Today and Would Be Costly to Implement.

The *Notice* seeks comment on ways to ensure that all alerts are properly authenticated and validated to protect against malicious or accidental misuse of alerting systems. It asks whether it should require EAS Participants to process and validate digital signatures when handling CAP-formatted EAS alerts, and to discard any CAP messages that do not match an authorized source from the Federal Emergency Management Agency (FEMA) or from a designated state source. It also seeks comment on how to authenticate traditional analog EAS messages using the EAS protocol. In addition, the Commission seeks comment on amending its rules to include a year parameter in the alert time stamp to prevent outdated alerts from triggering an EAS event, and to require devices to transmit only valid alerts.²¹

While we understand that CAP digital signature inspection may be provided for in some EAS encoder/decoder equipment, further research is needed to understand the extent to which it has been implemented. Further modifications to this equipment may be necessary. But with regard to the validation and authentication of *analog* EAS alert messages (as well as the addition of more header codes), it is not technically feasible for operators to implement the novel proposals in the *Notice* at this time as this would require extensive modifications by EAS

²¹ See *Notice* ¶¶ 140-45.

equipment manufacturers in conjunction with standards work, analysis and testing in the lab and in the field by EAS Participants, EAS equipment manufacturers, and FEMA.

The complicated nature of increasing the level of authentication and validation of analog EAS alerts requires greater study. But there is no question that adding these new functions will impose significant costs on cable operators who would have to install new firmware or software or replace EAS equipment altogether to meet these requirements.²²

II. THE COMMISSION SHOULD STREAMLINE THE PROPOSALS IT CONSIDERS IN DEVELOPMENT OF ANY VOLUNTARY INDUSTRY ROADMAP.

The *Notice* contains a lengthy discussion seeking input on how to “leverage technological advancements to improve the content, accessibility and security of emergency alerts” with the stated goal of initiating “a dialogue about creating a voluntary industry roadmap” for “further enhancing the nation’s alerting infrastructure” consistent with consumer expectations.²³ As EAS Participants, cable operators are committed to providing emergency alerts to their subscribers, and to utilizing new technological capabilities that become technically and operationally feasible. However, as explained herein, some of the approaches suggested in this portion of the *Notice* are problematic and should not be pursued as regulation, or even as part of a voluntary industry

²² In the discussion about community-based alerting exercises, the *Notice* seeks comment on authorizing periodic EAS exercises using live event header codes. *See Notice* ¶¶ 59-64. The Commission notes that use of live code testing may provide an opportunity to enable “more realistic system verification,” but it would also burden downstream EAS Participants by requiring costly communications to prevent public confusion prior to and during such a test. *See id.* ¶¶ 60-61. Using live EAS header codes and the EAS audio Attention Signal to conduct public awareness exercises should continue to require a waiver of Section 11.31(c). Because live code testing would distribute EAS messages lacking header information indicating that the activation is a test, viewers would need to be notified ahead of time – and outside of the EAS system itself – that the notification is not a real emergency. This would likely involve costly communications to cable customers (*e.g.*, via advertisements or bill inserts). The current waiver approach is preferable because it helps to put all involved entities on notice. If the Commission revises its rules to allow live code testing to occur absent a waiver request, it must minimize the burden on cable operators by requiring all downstream EAS stakeholders to be notified well ahead of the test and given the opportunity to choose not to participate.

²³ *See Notice* ¶¶ 75-96.

roadmap. Instead, the Commission should focus its efforts on examining an EAS alert delivery system that utilizes both IP and traditional approaches, as described in Section III, below.

A. New EAS Proposals That Would Fundamentally Alter Existing Cable EAS Infrastructure Are Not Viable.

The Commission should not pursue rules changes that would fundamentally alter the current EAS regime as it applies to cable operators providing video service. In particular, the Commission should preserve its current approach that utilizes force tuning, allows for selective override only where technically feasible and appropriate, and governs delivery of EAS alerts on “programmed channels” as that phrase is understood today. Any plausible public interest benefits served by altering these fundamental aspects of the current EAS regime would be outweighed by the significant costs and burdens imposed.

Force Tuning. We are particularly concerned about language in the *Notice* seeking comment on whether the Commission should fundamentally reconstruct how cable operators comply with EAS by abruptly abandoning the force tuning provisions of the current EAS regulatory regime.²⁴ Revising the rules in this way is not feasible – it would require a massive undertaking by cable operators, and would provide little, if any, benefit to consumers.²⁵

The EAS force tuning rules, as the Commission explains, allow cable operators “to transmit EAS audio and visual information over all channels by automatically tuning the subscribers’ set top boxes (STB) to a designated channel . . . that carries the required audio and

²⁴ See *id.* ¶ 84 (asking whether it should no longer “allow[] cable service providers to satisfy their requirements to transmit EAS audio and visual information by force tuning” and whether an “immediate (“flash cut”) elimination” of the “force tuning option” would create “any avoidable or unnecessary hardships”).

²⁵ Cable operators seamlessly convey thousands and thousands of EAS messages to subscribers using force tuning. Although the *Notice* cites a few instances where set-top boxes have frozen after force tuning an EAS alert, see *Notice* ¶ 78, these are isolated cases, not a systemic issue. To the extent the recent nationwide test revealed technical glitches, it served its purpose and operators have taken lessons learned from the test in those few instances to improve the system.

video EAS message.”²⁶ Force tuning is one of the primary components of how cable systems comply with EAS obligations. The Commission explained in 2005 that it would “permit digital cable systems that are participating in EAS activations to determine the method they will use to distribute EAS messages to viewers of digital cable channels as long as all viewers receive the complete EAS message on the channel that they are watching” and specifically recognized that “digital cable systems may transmit EAS messages on all digital channels or transmit EAS messages on a single channel and force tune all receivers to that channel.”²⁷ Consistent with this decision, cable operators have developed their EAS systems based upon the ability to force tune. Indeed, industry standards for emergency messaging rely upon force tuning, and are supported by millions of deployed set-top boxes and third party devices.²⁸

Dramatically changing course to disallow force-tuning in the EAS rules would require a massive overhaul of cable operators’ video networks and would include, among other things, EAS software and hardware components, including EAS encoders/decoders, set-top control equipment, and set-top boxes. The *Notice* lacks any basis for such a fundamental change to the current EAS, which would result in higher costs being passed along to consumers, and would not be in the public interest.²⁹ In addition, the software in many older set-top boxes is no longer being updated, making changes to those platforms time-consuming and costly.

²⁶ *Notice* ¶ 76 (referencing 47 C.F.R. § 11.51(g)(5), (h)(5)).

²⁷ *In re Review of the Emergency Alert System*, First Report & Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 18625 ¶ 32 & n.81 (2005).

²⁸ *See, e.g.*, ANSI/SCTE 18 2007: “Emergency Alert Messaging for Cable”.

²⁹ The *Notice* states that “some parties maintain that force tuning via the STB is not the only way that MVPD EAS Participants can display EAS information.” *Notice* ¶ 81 & n.200. The letter cited in the *Notice* describes a demonstration of a purported “competitive navigation device solution” that utilized “licensed video feeds from two different MVPDs.” Letter from Angie Kronenberg, Chief Advocate & General Counsel, INCOMPAS, to Marlene H. Dortch, Secretary, FCC, MB Dkt. No. 15-64 at 1-2 (filed Dec. 14, 2015). The letter did not provide information on alternative technologies that can be deployed by MVPDs to deliver EAS alerts. We have little information about the demonstration, but, the demonstration sponsors later clarified that they simulated an EAS alert they claimed to be “of a standard nature.” They did not address the fact that MVPD networks use many

Selective Override. Within the same discussion, the *Notice* asks whether “selective override” should “remain an acceptable voluntary EAS alternative for cable systems.”³⁰ As an initial matter, it is inaccurate to describe selective override as “an acceptable voluntary EAS alternative” for cable systems. The EAS rules *require* cable operators to override the audio and video on *all* programmed channels, unless there is a written agreement with a broadcast station to not override that particular station.³¹ 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.³²

Cable operators consistently provide their subscribers with emergency alerts, whether originated by a broadcaster or a cable operator, and where feasible, operators utilize the non-override agreement provision of the EAS rules. Where cable operators have flexibility under their franchise agreements, where they have newer, upgraded equipment in place, and where it

different emergency alert protocols, not just the one simulated by Google. *See* Letter from Robert S. Schwartz, Counsel, Consumer Video Choice Coalition, to Marlene D. Dortch, Secretary, FCC, filed in MB Dkt. No. 15-64 & CS Dkt. No. 97-80, at 2 (Jan. 14, 2016). The participants in the demonstration refused to provide additional information on how to support EAS on these diverse networks.

³⁰ *Notice* ¶ 80.

³¹ *See* 47 C.F.R. § 11.51(g) (requiring “a video interruption and an audio alert message on all channels”) & (h). Selective override is not viable for many cable systems because it is not technically feasible for them, their franchising agreement restricts their ability to selectively override, and/or such an agreement is not appropriate for the particular area served by the cable system.

³² *See, e.g., In re Amendment of Part 73, Subpart G, of the Commission’s Rules Regarding the Emergency Broadcast System*, Third Report & Order, 14 FCC Rcd 1273, 1282 (1998); *In re Amendment of Part 11 of the Commission’s Rules Regarding the Emergency Alert System*, Report & Order, 17 FCC Rcd 4055 ¶ 77 (2002). As we have explained,

While many broadcast stations provide detailed emergency information, it is also the case that many stations have no news departments and hence do not provide coverage of emergency situations. And, in some instances cable systems provide local alerts unique to their service areas. In some smaller communities outside metropolitan areas, cable alerts are the only source of emergency information specific to those areas. Thus, adoption of [mandatory selective override] could result in a cable viewer watching a broadcast station on a cable system being deprived, in some cases, of *any* emergency information if the broadcaster does not provide it.

NCTA Reply Comments at 6, n.22, PS Dkt. No. 04-296 (filed Nov. 19, 2013).

benefits their customers, they have worked with broadcasters to omit their stations from all-channel EAS overrides.

The *Notice* asks how digital technologies, including “smart” set-top boxes, might affect the use of selective override.³³ As cable operators deploy more advanced set-top boxes, some of the costs to facilitate selective override may decrease, but the question does not simply hinge on set-top boxes. The delivery of EAS alerts requires many different software and hardware components in different parts of the cable plant. In addition, the decision to selectively override particular stations has to be consistent with a cable system’s local alerting needs and can only occur in the absence of any franchise-based all-channel emergency alerting requirements.

That said, any mandate to require *universal* selective override remains an ill-advised and burdensome proposition as a technical matter for cable operators. As we have previously explained:

While selective override technology has been developed, deploying it in a digital environment is a huge task given the complexity of supporting many set-top box platforms. The challenges include working with the many set-top box manufacturers to support this feature through software upgrades and interfacing the various platforms’ controlling systems with cable guide and billing systems. Moreover, in cable systems using more than one set-top box platform, instituting selective override must be accomplished in an all or nothing scenario. This is an expensive and resource-intensive process.³⁴

Furthermore, many set-top boxes and platforms are no longer being updated as cable operators focus on developing solutions for newer, more full-featured and competitive offerings. The selective override scheme designed by the Commission is working as intended. There is no technical or policy basis for the Commission to reexamine these rules yet again.

³³ See *Notice* ¶ 81.

³⁴ NCTA Reply Comments at 6-7, PS Dkt. No. 04-296 (filed Nov. 19, 2013).

Programmed Channels. Finally, the *Notice* asks if there is a technical basis to revise which channels are required by cable operators to carry EAS alerts to encompass, for example, all “channels that are made available for consumer use.”³⁵ Today, the Commission’s EAS rules apply to “programmed channels,” a term that, per the rules, specifically excludes channels used for the transmission of “data such as interactive games,” “data services such as Internet,” or data services such as Internet access.”³⁶ The Commission should preserve the existing approach for both legal and policy reasons.

The Cable Act of 1992 extended EAS obligations to cable operators, directing the Commission to promulgate regulations to “ensure [] viewers of *video programming* on cable systems” receive EAS alerts.³⁷ “Video programming,” in turn, is defined in the Act as that “provided by, or generally considered comparable to programming provided by, a television broadcast station.”³⁸ The Commission first used the phrase “programmed channel” in 1997, defining it as “a channel carrying video programming” and noting that “[c]hannels not used for video programming are not required to carry EAS messages or alerts.”³⁹ Thus, expanding the definition to cover “all channels that are part of the service package offered to the consumer” would exceed the Commission’s authority.

In any event, EAS systems deployed by cable operators are based upon the Commission’s current definition of a “programmed channel,” and, similar to proposals related to force tuning

³⁵ *Notice* ¶ 86.

³⁶ *Id.* ¶ 85, nn.202-04 (citing 47 C.F.R. § 11.11, Table 2 n.3, Table 3 n.4, & Table 4 n.4).

³⁷ Cable Act of 1992, Pub. L. No. 102-385, § 16(b) (codified at 47 U.S.C. § 544(g)) (emphasis added); *see also* *Notice* ¶ 184 (referencing § 624(g) of the Act).

³⁸ 47 U.S.C. § 522(20).

³⁹ *In re Amendment of Part 73, Subpart G, of the Commission’s Rules Regarding the Emergency Broadcast System*, Second Report & Order, 12 FCC Rcd 15503 ¶ 38 (1997).

and selective override, expanding that definition would have significant technical implications for cable EAS infrastructure and should not be pursued.

* * *

In sum, the potential benefit of adopting rules that would significantly disrupt how cable operators comply with their EAS obligations today is unclear, particularly in light of the Commission’s recognition that other alerting technologies serve many of the same purposes and are already available to consumers.⁴⁰ It simply does not make sense for the Commission to go down a path of fundamentally recreating the EAS obligations currently applicable to cable systems.

B. The Commission Should Not Explore Disparate Regulatory Treatment of EAS Participants Offering OTT Services.

In an effort to “initiate a conversation regarding how the EAS may remain durable as the ways in which consumers view content evolves,” the *Notice* seeks comment on “the extent to which EAS Participants offer [OTT] versions of their broadcast, cable and other services” and “what technical, policy or jurisdictional issues would need to be addressed in order to make EAS available over such services.”⁴¹ We appreciate the Commission’s efforts to “initiate a conversation,” but caution against an unnecessary and legally questionable rush to impose EAS requirements on OTT video services offered by EAS Participants.

As a preliminary matter, the Commission’s questions in this area appear to reflect some confusion between digital cable services delivered via IP on a managed basis by cable operators,

⁴⁰ As the *Notice* suggests, new technologies may offer benefits for the future of emergency alerting that current traditional video platforms lack. *See, e.g., Notice* ¶ 9 (describing success of the Commission’s voluntary mobile-subscriber alerting program (WEA), which has delivered 21,000 emergency alerts to mobile devices since April 2012); ¶ 11 (explaining that social media platforms, including Google, Twitter, and Facebook, are increasingly used as alerting tools and offer unique benefits including interactivity and personalization); ¶ 89 n.211 (noting that online services can geographically tailor alerts more easily).

⁴¹ *Id.* ¶¶ 3, 88.

which are *already* subject to certain EAS requirements, and video services delivered over the Internet, which are not.⁴² For example, the *Notice* explains that a “wealth of video content is now available to consumers online,” and then adds, by way of example, that MVPDs “are beginning to offer IP-based versions of their programming, including providing consumers with apps to view content.”⁴³ The implication appears to be that MVPD apps are receiving video over-the-top of an Internet connection. However, cable service can be delivered in IP format to operator-supplied set-top boxes in the home, or to cable apps that customers download to their tablets, smartphones, and other IP-capable devices.⁴⁴ Whether 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.⁴⁵ In contrast, video that is delivered in IP on the public Internet does not support EAS.

In any event, it is not clear that the Commission has authority to extend EAS obligations to *any* provider of video services delivered “over-the-top,”⁴⁶ and there would be no rational basis to distinguish between OTT video services offered by EAS Participants and those offered by

⁴² See 47 C.F.R. § 11.11(a) (identifying among other EAS participants “analog cable systems” and “digital cable systems, which are defined for purposes of this part *only as the portion of a cable system that delivers channels in digital format to subscribers at the input of a Unidirectional Digital Cable Product or other navigation device*”) (emphasis added).

⁴³ *Notice* ¶ 88.

⁴⁴ The Commission has recognized that cable service delivered in IP is treated as cable service under the Communications Act. See, e.g., *In re Promoting Innovation and Competition in the Provision of Multichannel Video Programming Distrib. Serv.*, Notice of Proposed Rulemaking, 29 FCC Rcd 15995 ¶ 74 (2014) (noting “an entity that delivers cable services via IP is a cable operator to the extent it delivers those services as managed video services over its own facilities and within its footprint” while services like “TV Everywhere” do not qualify as cable services because “they are not managed video services”); *In re Closed Captioning of Internet Protocol-Delivered Video Programming: Implementation of the [CVAA]*, Report & Order, 27 FCC Rcd 787 ¶ 11 (2012) (clarifying that “the new IP closed captioning rules do not apply to traditional managed video services that MVPDs provide to their MVPD customers within their service footprint, regardless of the transmission protocol used”).

⁴⁵ Cable apps today are designed to support EAS. See Final Report of DSTAC at 42-43, MB Dkt. No. 16-42, available at <http://apps.fcc.gov/ecfs/document/view?id=60001515603>; NCTA Comments, MB Dkt. No. 16-42, CS Dkt. No. 97-80, at 86 (filed Apr. 22, 2016); Comcast Corp., Opposition at 12, MB Dkt. No. 10-56; GN Dkt. No. 14-28 (filed Mar. 14, 2016).

⁴⁶ See *Notice* ¶ 184 & nn.307-08, 310 (referencing 47 U.S.C. §§ 151, 154(i) and (o), 303(r), 544(g), 606, & 613 as providing the Commission legal authority to require emergency alerts).

other entities such as Netflix and Amazon. If the Commission claims jurisdiction to regulate the OTT video services of EAS Participants, it would effectively be asserting jurisdiction over *all* OTT video services, and there is no legal or policy basis to impose disparate alerting obligations on an arbitrary subset of online video providers.

The plain language of Section 624(g) directs the Commission “to ensure that viewers of *video programming on cable systems* are afforded the same emergency information as is afforded by the emergency broadcasting system.”⁴⁷ The Commission has construed this provision to apply to DBS providers and certain other MVPDs, but even that interpretation stops well short of covering online video services that deliver content over the Internet.⁴⁸ None of the other provisions referenced in the *Notice* has any direct connection to EAS, let alone to emergency alerting obligations for OTT video services, regardless of whether a provider is an EAS Participant with respect to other services.⁴⁹

⁴⁷ 47 U.S.C. § 544(g) (emphasis added). As noted herein, the Commission has recognized the difference between cable services subject to Title VI, and video services delivered over the Internet. *See supra* note 44. Section 624(g) deals exclusively with the former, and cannot be invoked to regulate OTT video providers.

⁴⁸ *See In re Review of the Emergency Alert System*, First Report & Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 18625 ¶ 54 n.173 (2005) (requiring DBS providers to participate in national EAS activations and pass through EAS messages aired on local channels). Similarly, Section 613, a provision of the CVAA, pertains to accessibility of emergency information by individuals who are blind or visually impaired but does not include language suggesting Congressional intent to impose new emergency alerting obligations on any platform.

⁴⁹ Sections 1 and 4(o) of the Act do not independently confer regulatory authority. *See Comcast Corp. v. FCC*, 600 F.3d 642, 652-54 (D.C. Cir. 2010). Section 706 is problematic for a number of reasons, including that it cannot provide the statutory basis for EAS rules that the Commission would otherwise lack authority to adopt. *See* 47 U.S.C. § 606(g) (“Nothing in subsection (c) or (d) of this section shall be construed to authorize the President to make any amendment to the rules and regulations of the Commission which the Commission would not be authorized by law to make.”). Sections 4(i) and 303(r) are “more akin to a ‘necessary and proper’ clause” than stand-alone sources of authority and must be invoked in a manner “reasonably ancillary” to the Commission’s expressly delegated functions. *See Motion Picture Ass’n of Am. v. FCC*, 309 F.3d 796, 806 (D.C. Cir. 2002). To the extent the Commission would rely on ancillary authority, there is nothing in the Communications Act that would create such “statutorily mandated responsibilities” with respect to OTT video services or provide a reasonable basis to extend EAS requirements to such services. *See Am. Library Ass’n v. FCC*, 406 F.3d 689, 692-93 (D.C. Cir. 2005).

Moreover, interpreting any of these provisions to impose EAS obligations on OTT video services would also conflict with repeated assurances that the Commission does not intend to “regulat[e] the Internet, *per se*, or any Internet applications or content.”⁵⁰ The Wireline Competition Bureau recently reaffirmed that the Commission “has been unequivocal in declaring that it has no intent to regulate edge providers.”⁵¹

There is also no need to apply existing EAS obligations to OTT video services. 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. The same is true for radio and television broadcasts, which are also delivered locally. There is no similar expectation for OTT services which can be accessed anywhere via any Internet connection. A consumer who resides in Washington, DC, for example, doesn’t receive, or expect to receive alert information unique to that region while accessing OTT video from Netflix, iTunes, and Amazon Prime. To the extent that consumers have an interest in receiving emergency alerts while online, alternative alerting mechanisms already exist to meet that need, including through their mobile phones, social media, and the Internet.⁵²

⁵⁰ *In re Protecting and Promoting the Open Internet*, Report & Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 ¶ 382 (2015); *see also id.* ¶ 282 n.725 (emphasizing that “today’s rules apply only to last-mile broadband providers” and rejecting suggestions that the Commission’s decision “could be read to impose regulations on edge providers or others in the Internet ecosystem”).

⁵¹ *In re Consumer Watchdog Petition for Rulemaking to Require Edge Providers to Honor ‘Do Not Track’ Requests*, Order, 30 FCC Rcd 12424 ¶ 1 (WCB 2015).

⁵² Today consumers have the option to receive geographically-targeted alerts on mobile devices. *See* FCC, Wireless Emergency Alerts (WEA), <https://www.fcc.gov/consumers/guides/wireless-emergency-alerts-wea>. There is also a wide variety of emergency information available via social media and the Internet. For example in the Washington, DC metro area, many local jurisdictions offer emergency alerts delivered by email and/or text message. *See, e.g.*, AlertDC, <http://hsema.dc.gov/page/alertdc>; Alert Montgomery, <https://member.everbridge.net/index/1332612387832009#/faq>; Arlington Alert, <http://departments.arlingtonva.us/oem/>; Fairfax Alerts, <http://www.fairfaxcounty.gov/alerts/>. Additionally,

If the Commission would somehow nevertheless conclude that it should regulate only the OTT video services of EAS Participants, such a fragmented approach would be counterproductive, creating consumer confusion through piecemeal access to emergency information. There is no sound technical basis or public safety rationale for an EAS mandate that would apply to the OTT offerings of broadcasters and MVPDs, but not to other OTT video services like Netflix, Amazon Prime, or iTunes. Moreover, such a regulatory approach would create an uneven playing field in the market for OTT video services, harming competition and deterring innovation by subjecting certain providers to regulatory burdens that would not apply to their competitors. In sum, imposing disproportionate EAS requirements on the OTT video services of EAS Participants would do little to protect public safety, would violate basic requirements of “reasoned decisionmaking,”⁵³ and would be arbitrary, capricious, and contrary to law.⁵⁴

C. New Translation or Accessibility Requirements Are Unnecessary.

The *Notice* seeks comment on potential improvements in accessibility, focusing on “the state of technology for machine-generated translation.”⁵⁵ At this time, consideration of any rule on the issue of providing multilingual EAS messages, or even provisions for a voluntary industry roadmap, are unnecessary, and in any event, would be premature. Indeed, the Commission

alerting authorities from 15 states, the District of Columbia, the U.S. Virgin Islands, FEMA, and a number of other federal agencies are participating organizations in Twitter’s emergency alerts platform. *See* Twitter Alerts, Participating Organizations, at <https://about.twitter.com/products/alerts/participating-organizations> (last visited June 7, 2016); New York City Emergency Alerts, Twitter, at <https://twitter.com/notifynyc>. Many other local governments leverage Facebook and other social media tools to issue alerts and disseminate emergency information. *See, e.g.*, Los Angeles County Office of Emergency Management, Facebook, at <https://www.facebook.com/Los-Angeles-County-Office-of-Emergency-Management-159497677486291/>.

⁵³ *Allentown Mack Sales & Service, Inc. v. NLRB*, 522 U.S. 359, 374 (1998).

⁵⁴ *See Motor Vehicle Mfrs. Assn. of United States, Inc. v. State Farm Mut. Automobile Ins. Co.*, 463 U.S. 29, 43 (1983) (agencies may not “entirely fail[]to consider an important aspect of the problem, offer[]an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise”).

⁵⁵ *Notice* ¶ 94.

considered multilingual EAS alerts in a recent Order, and appropriately concluded that alert originators – not cable operators or other EAS participants – are best positioned to determine when it make sense to issue alerts in multiple languages.⁵⁶ However, as suggested in the *Notice*, the Commission could assign an examination of the status of machine-generated translation to an advisory committee in the event that new rules should be considered at some point in the future.⁵⁷

III. THE COMMISSION SHOULD CONVENE A MULTI-STAKEHOLDER INITIATIVE TO CONSIDER THE MIGRATION TO PRIMARY IP DELIVERY OF EAS ALERTS.

The *Notice* asks if the Commission needs to engage in a “wholesale rethinking of the alerting system.”⁵⁸ Relatedly, the *Notice* asks if “it make[s] sense to migrate to one system” instead of preserving dissemination of EAS alerts on the legacy daisy chain alongside delivery in IP via IPAWS.⁵⁹ The cable industry would welcome the opportunity to collaborate with the Commission, EAS participants, and other interested stakeholders on a task force to modernize EAS by further embracing the IPAWS approach and migrating toward primary delivery of EAS alerts to EAS Participants via IP capability. As discussed above, the Commission’s inquiry

⁵⁶ See *In re Review of the Emergency Alert System; Ind. Spanish Broad. Ass’n, the Office of Commc’n of the United Church of Christ, and MMTC, Petition for Immediate Relief; Randy Gehman Petition for Rulemaking*, Order, 31 FCC Rcd 2414 ¶ 20 (2016) (“We agree with the majority of commenters that alert originators are best positioned to effect multilingual alerting, since station operators simply pass down the EAS message as received within the allotted two minute timeframe and, by and large, do not have the necessary capabilities and/or time to translate or originate that alert in another language.”). This decision is consistent with NCTA’s advocacy on this issue. See, e.g., NCTA Comments, EB Dkt. No. 04-296 at 2 (filed May 28, 2014); NCTA Comments, EB Dkt. No. 04-296 at 5 (filed May 17, 2010) (“[C]able operators simply pass the EAS message through in the two-minute window as received and generally do not have the capability to create or translate the message into additional languages.”).

⁵⁷ See *Notice* ¶ 75 n.190 (“Apart from the proposals set forth in this *Notice*, other initiatives to facilitate this dialogue could include reference to an advisory committee for further consideration or a workshop on the issue conducted by PSHSB.”). We also note that a CSRIC working group is in the midst of studying this very issue. See CSRIC V Working Group, Descriptions and Leadership, at 2-3 (Aug. 4, 2015), available at <https://www.fcc.gov/file/3465/download>.

⁵⁸ *Notice* ¶ 175.

⁵⁹ *Id.* ¶ 176.

should be focused on improving and modernizing EAS itself, not on a counterproductive and legally unsustainable effort to mandate EAS participation across all devices and services that use IP technology.

The broadcast daisy chain approach to EAS is robust and vital, especially if a catastrophic event diminishes IP capability. However, transitioning to primary IP EAS alert delivery would be consistent with recent Congressional action,⁶⁰ and might better serve the public interest as a primary mode to transmit alerts (with the legacy daisy chain providing secondary alert delivery). IP may provide an opportunity to deliver alerts faster and more efficiently than the daisy chain by distributing alerts to all EAS Participants at once.⁶¹ IP alerts may also be more effective, containing pictures and information beyond what is capable of being delivered via basic text scrolls and allowing for more precise geo-targeting than currently exists. IP alerts may also provide greater security protections in order to prevent unauthorized access and false alerts. And, if properly engineered, a primary IP infrastructure (especially when paired with secondary delivery via the daisy chain) can satisfy the Commission's concerns about EAS transmission redundancy and resiliency.⁶²

To modernize EAS, the Commission should consider convening a multi-stakeholder initiative to facilitate the migration of EAS to a primary IP environment. This approach would be consistent with the Commission's previous use of advisory committees and other multi-

⁶⁰ Congress recently passed the IPAWS Act, which directs FEMA to modernize IPAWS for more effective delivery of EAS alerts. *See* Integrated Public Alert and Warning System Modernization Act of 2016, Pub. L. No. 114-143 (Apr. 11, 2016) ("IPAWS Act").

⁶¹ *See Public Safety & Homeland Security Bureau Seeks Comment on Ways to Facilitate Earthquake-Related Emergency Alerts*, Public Notice, DA 16-380 (rel. Apr. 8, 2016) (seeking input for a report to Congress on an alerting system utilizing IPAWS to distribute earthquake-related emergency alerts in fewer than three seconds).

⁶² *See Notice ¶¶ 175-78; see also In re Review of the Emergency Alert Sys.; Indep. Spanish Broad. Ass'n, the Office of Comm. of the United Church of Christ, and the Minority Media & Telecomm. Council, Petition for Immediate Relief*, Order, FCC 16-32 (rel. Mar. 30, 2016) (observing the legacy system's ability to provide alerts to the public even after damage to the electrical power grid). Congress tasked FEMA with modernizing IPAWS to address this concern. *See* IPAWS Act § 526(b)(5).

stakeholder efforts to inform its consideration of long-term EAS issues.⁶³ The Commission, FEMA, state and local governments, alert originators, MVPDs, broadcasters, equipment vendors, accessibility groups, and other interested stakeholders should all be involved in considering the complex technical and policy challenges associated with such an eventual migration and developing actionable recommendations for the Commission.

CONCLUSION

The Commission should reevaluate its EAS proposals consistent with the foregoing. Instead of imposing new ad hoc rules on EAS participants, the Commission should convene a multi-stakeholder initiative to address EAS modernization.

Respectfully submitted,

/s/ Rick Chessen

William A. Check, Ph.D.
Senior Vice President, Science & Technology
Chief Technology Officer

Andy Scott
Vice President, Engineering
Science & Technology

June 8, 2016

Rick Chessen
Loretta Polk
Stephanie L. Poday
National Cable & Telecommunications
Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

⁶³ See, e.g., Charter of the Communications Security, Reliability, & Interoperability Council (CSRIC) (Mar. 19, 2015), available at https://transition.fcc.gov/bureaus/pshs/advisory/csric5/CSRIC_Charter_Renewal_2014.pdf (directing CSRIC V to “[d]evelop recommendations for actions the FCC should take to enhance the ability of the public to receive timely and accurate emergency alerts and warnings, including ways to leverage advanced communications technologies and the Internet, including broadband technologies and social media platforms”); *In re Review of the Emergency Alert Sys.; Indep. Spanish Broad. Ass’n et al. Petition for Immediate Relief*, Second Report & Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 13275 ¶ 72 (2007) (directing the Public Safety and Homeland Security Bureau “to convene a meeting – or series of meetings – as soon as possible concerning EAS as it relates to the needs of non-English speakers” and to “submit into the record a progress report on these discussions”).