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

In the Matter 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 NCTA – THE INTERNET & TELEVISION ASSOCIATION

Andy Scott
Vice President, Engineering Technology

Rick Chessen
Loretta Polk

NCTA – The Internet & Television Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

September 10, 2018

TABLE OF CONTENTS

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

In the Matter 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 NCTA – THE INTERNET & TELEVISION ASSOCIATION

NCTA – The Internet & Television Association ("NCTA")[1] respectfully submits these comments in response to the Further Notice of Proposed Rulemaking in the above-captioned proceedings.[2]

INTRODUCTION AND SUMMARY

As an integral part of the Emergency Alert System ("EAS"), NCTA's cable operator members share the Commission's goals of promoting public confidence in EAS and preventing false alerts. But as the Commission considers a regulatory response to the false missile alert in Hawaii in January, it should bear in mind that cable operators are passive conduits for alerts generated upstream in the EAS architecture and transmit state and local alerts on a voluntary basis. The Hawaii incident called attention to the confusion and public safety risks associated with false alerts, but it did not involve any error or omission by cable operators or other EAS

---

1 NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving approximately 85 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 more than $250 billion over the last two decades to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to more than 30 million customers.

2 *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System; Wireless Emergency Alerts*, Report and Order and Further Notice of Proposed Rulemaking, -- FCC Rcd -- (2018) ("*Report and Order*" or "*Further Notice*," as appropriate).

Participants. While it is understandable for the FCC to seek comment on actions within its jurisdiction to address failures in Hawaii, increased regulation of EAS Participants is not a solution to problems better resolved by the Federal Emergency Management Agency ("FEMA") and state and local authorities with direct responsibility for alert origination. Instead of revisiting unnecessary regulatory proposals from a 2016 Notice of Proposed Rulemaking ("NPRM"), the Commission should continue working with other EAS stakeholders on more efficient solutions that impose fewer burdens on communications providers.[3]

The Commission has recognized that the communications networks and equipment that transmitted the Hawaii alert functioned properly despite "a combination of human error and inadequate safeguards" on the part of alert originators at the Hawaii Emergency Management Agency ("HI-EMA").[4] As the *Hawaii Report* makes clear:

> Neither the false alert nor the 38-minute delay to correct the false alert would have occurred had Hawaii implemented reasonable safeguards and protocols before January 13, 2018, to minimize the risk that HI-EMA would issue a false alert, and to ensure that HI-EMA would be able to issue a rapid correction of any false alert that was delivered to the public.[5]

Consistent with these findings, a PSHSB official testified in Congressional field hearings that "[t]he majority of EAS participants received the alert within seconds and retransmitted it," and "[f]rom a technical perspective, this was exactly as the system is designed to work."[6] And as

---

3 *See 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) ("*2016 NPRM*").

4 FCC Public Safety and Homeland Security Bureau, Report and Recommendations: Hawaii Emergency Management Agency January 13, 2018 False Alert, ¶ 6 (April 2018) ("*Hawaii Report*").

5 *Id.*

6 Written Statement of Nicole McGinnis, Deputy Chief, PSHSB, "Hawaii False Missile Alert: What Happened and What Should We Do Next?" Before the Senate Committee on Commerce, Science and Transportation, at 2 (April 5, 2018).

Commissioner O'Rielly observed in response to the *Further Notice*, "the near-catastrophic mistake in Hawaii was the fault of a delusional individual" that "does not justify new burdens on the private sector that did nothing wrong."[7]

The Commission's recent decision to require EAS Participants to send an email to the FCC Ops Center within 24 hours of having "actual knowledge" of a false alert is problematic. In contrast, other proposals in the *Further Notice* could provide the Commission with more useful information and should be pursued. NCTA urges the Commission to use the *Further Notice* to revise the false alert reporting mandate that it adopted in July to encourage reporting by alert originators and other entities in a better position to detect and respond to false alerts. In addition, the Commission should:

- Decline to impose any further false alert reporting requirements for EAS Participants;
- Reject the unnecessary proposal to establish a reporting system for set-top box "lockouts" that prevent tuning back to other programming once an EAS alert has concluded; and
- Provide a strong presumption of confidential treatment for any proprietary, competitively sensitive information that may be contained in any reports that the Commission does require.

Beyond these changes, the Commission should continue to work with FEMA and state and local emergency authorities on EAS issues that extend beyond the FCC's jurisdiction over communications providers. For example, the Commission can address any further concerns about false alerts by requiring State EAS Plans to include procedures to prevent and correct such incidents. Emergency managers and alert originators – not cable operators or other EAS

[7] *Further Notice*, Statement of Commissioner O'Rielly.

Participants – may be better equipped to develop and implement best practices or other guidance to prevent or mitigate the harms that the *Further Notice* seeks to address.[8]

I. THE COMMISSION SHOULD REVISE ITS FALSE ALERT REPORTING RULE AND DECLINE TO ADOPT ADDITIONAL FALSE ALERT REPORTING REQUIREMENTS

To the extent it continues to require some form of false alert reporting, the Commission should incorporate proposals from the *Further Notice* to gather more useful information from a broader range of stakeholders without imposing unwarranted regulatory burdens on EAS Participants. As NCTA and others explained in 2016, cable systems are passive conduits of EAS messages generated by alert originators and transmitted by upstream EAS equipment.[9] Because of their role in the EAS architecture, cable operators are in no position to independently verify the accuracy of each EAS activation. If cable system equipment receives a properly formatted EAS message and is configured to transmit that event code, it will display the corresponding alert without any human intervention or subjective judgement as to whether the alert was issued in error. This is not a coincidence or a flaw in the system, but an inherent characteristic of an automated, hierarchical EAS designed to transmit alerts from originators to cable subscribers as quickly as possible.[10]

---

8 *See* Testimony of Lisa M. Fowlkes, Chief, PSHSB, Before the Senate Commerce, Science and Transportation Committee, at 33:18 (Jan. 25, 2018), https://www.c-span.org/video/?440246-1/hearing-focuses-effectiveness-emergency-alert-system&start=5232 (stating in response to a question from Sen. Thune that "[t]he FCC is responsible for the distribution part of the EAS," and that "we do not have authority over the alert origination piece").

9 *See* NCTA Comments, PS Docket No. 15-94 at 8 (June 8, 2016) ("*NCTA 2016 Comments*") (noting that "[c]able operators disseminate EAS alerts on an automated basis, often from facilities that are not staffed 24 hours per day," and that "operators have no way to determine that an EAS transmission is false using current equipment").

10 If anything, the *Hawaii Report* appears to fault certain EAS Participants for not configuring equipment to "auto-forward" the particular EAS codes used to transmit the false alert and subsequent correction. *See Hawaii Report* ¶ 29. Putting aside the voluntary nature of such non-Presidential EAS event codes, the report's emphasis on "auto-forwarding" underscores that cable operators transmit EAS messages on an automated basis and would have no way of knowing if a particular alert is "false."

Against this backdrop, it remains unclear what kind of information the Commission expects to receive in emails from EAS Participants reporting false alerts, or how a reporting mandate limited to communications providers will "help ensure that the Commission, FEMA and affected stakeholders have sufficient information to identify and mitigate problems with the EAS," as the *Further Notice* asserts.[11] In the 24 hours following the Hawaii incident, for example, EAS Participants had no more information about the false missile alert than the news reports and social media available to the general public. The most that any cable operator could have reported to the FCC under the circumstances was that, according to state officials and news reports, the missile alert issued by HI-EMA was a false alarm, and that alert was transmitted to the operator's subscribers.[12]

Although the *Report and Order* characterizes its 24-hour email reporting requirement as "minimally burdensome," it raises practical questions that will make compliance far more difficult and confusing than the Commission suggests. Is a "false alert" one generated by an EAS Participant's own personnel or equipment (e.g., through human error or equipment/software malfunction), or are cable operators responsible for reporting the falsity of alerts issued by third parties (e.g., the missile alert in Hawaii)? What constitutes "actual knowledge" that an alert is false, and must EAS Participants independently investigate the circumstances surrounding each

---

[11] *Further Notice* ¶ 40.

[12] It is worth noting that bipartisan legislation currently pending in Congress would direct the FCC, in consultation with FEMA, to "complete a rulemaking proceeding to establish a system to receive *from the [FEMA] Administrator or State, Tribal, or local governments* reports of false alerts . . . for the purpose of recording such false alerts and examining their causes." *See* Reliable Emergency Alert Distribution Improvement Act of 2018 (READI Act), S. 3238, § 6, 115th Congress (2017-2018), https://www.congress.gov/bill/115th-congress/senate-bill/3238/text (emphasis added). The approach proposed in the READI Act would provide the FCC with more useful information by focusing on reporting by the alert originators who are likely to have first-hand knowledge of any false alerts rather than downstream EAS Participants that merely transmit the resulting alert messages.

alert they transmit? Would news reports or other publicly available information about a false alert obligate EAS Participants to report transmission of that alert to the FCC?

The *Further Notice* proposes a better approach by asking whether, "in lieu of adopting a dedicated reporting mechanism for false EAS or WEA alerts or EAS lockouts, [the FCC] should instead implement a process by which EAS Participants, Participating CMS Providers, emergency managers, and members of the public could inform the Commission about false alerts through currently available means," such as the Commission's existing Public Safety Support Center reporting portal.[13] In NCTA's view, it is essential that any false alert reporting regime reach this broader range of stakeholders – particularly alert originators – rather than inappropriately relying on EAS Participants to report events beyond their direct knowledge or control. The most efficient and least burdensome option would be for EAS stakeholders of all types to email the FCC Ops Center or visit the online Public Safety Support Center, on a voluntary basis, whenever they may have relevant information about a false alert, and not burden the Commission with duplicative mandatory reports of little practical value. If, however, the Commission continues to require EAS Participants to email the Ops Center within 24 hours of having "actual knowledge" of a false alert, it should at least make clear that the same reporting mechanism is available to other entities that may be in a far better position to provide the information the Commission is looking for.[14]

---

[13] *Further Notice* ¶ 41 (discussing the FCC's online Public Safety Support Center, https://www.fcc.gov/general/public-safety-support-center).

[14] NCTA recognizes that jurisdictional issues may limit the Commission's ability to adopt rules compelling other government entities to report false alerts, but the FCC can still play a constructive role by strongly encouraging *all* EAS stakeholders, including federal, state, and local emergency authorities, to participate in any reporting regime it decides to adopt. It would not be good law or policy to limit reporting obligations to EAS Participants simply because the Commission lacks regulatory jurisdiction over other entities with more useful information.

In any event, the Commission should reject the additional false alert reporting mandates proposed in the *Further Notice*. There is no need – or practical use – for a "dedicated reporting mechanism" beyond the email notification the FCC has already decided to require, particularly any reporting regime targeted solely at EAS Participants.[15] As NCTA and others explained in 2016, mandatory reporting on timeframes as short as five minutes is simply not feasible, let alone a wise use of resources.[16] A dedicated reporting system, mandatory form fields, and other "reporting parameters" discussed in the *Further Notice* would only divert attention away from efforts to work with alert originators and emergency authorities to correct and mitigate public confusion resulting from any future false alerts. If anything, the *Further Notice* appears to recognize the risks of further duplication and confusion through questions about geographic overlap and the possibility of "receiving different descriptions, times, locations and reporting identities covering the same false alert."[17] A single, clearly identifiable error triggering a false alert, as occurred in the Hawaii or "Bobby Bones Show" examples discussed in the *Further Notice*, could easily result in redundant investigation and reporting by hundreds of EAS Participants.[18] The Commission should avoid creating problems of its own making and decline to adopt these proposals.

---

15 *Further Notice* ¶ 40.

16 *See* NCTA Reply Comments, PS Docket No. 15-94 at 6 (July 8, 2016) ("*NCTA 2016 Reply Comments*") ("The proposed rule would place operators in the untenable position of second-guessing the validity of every alert they receive or facing penalties for failing to report an alert that is later found to be initiated without proper authorization.").

17 *Further Notice* ¶ 41.

18 *See id.* ¶ 38 n.103 (estimating that 290 EAS Participants would have been required to report the "Bobby Bones Show" incident, "assuming all 290 entities had actual knowledge they had transmitted a false alert"); *see also Turner Broadcasting System, Inc.*, Notice of Apparent Liability for Forfeiture, 28 FCC Rcd 15455 ¶ 7 (2013) (assessing forfeiture for TBS Network's transmission of a false EAS alert in a promotion for the "Conan" show to MVPDs "throughout the country").

II. THE COMMISSION SHOULD NOT MANDATE REPORTING OF LOCKOUTS

Given the lack of record support for the *2016 NPRM's* lockout reporting proposals, it is not clear why the *Further Notice* revisits this unnecessary proposed obligation.[19] There were no lockouts reported in connection with the Hawaii incident, and the failures revealed by PSHSB's investigation had nothing to do with cable equipment or inability to tune back to regularly scheduled programming.

Notwithstanding the isolated lockout events discussed in the *2016 NPRM*, many of the causes of past lockouts have already been resolved through software updates and improvements in cable equipment. There is no reason to expect that lockouts will be a significant issue for cable subscribers in the future, and no reasonable basis to adopt an additional reporting requirement. And even if some lockouts may occur in the future, it is still not clear what purpose a dedicated reporting mechanism would serve. Neither the *2016 NPRM* nor the *Further Notice* explains how reporting to the FCC would actually assist in any response activities or make any meaningful difference to cable subscribers. Cable operators have every incentive – both from a network management and customer service perspective – to prevent and mitigate the impact of any lockouts affecting their subscribers, and the industry has already acted to address the causes of past lockouts and will continue to address any issues without further action by the Commission.

---

[19] *See NCTA 2016 Reply Comments* at 5 ("Multiple commenters confirm that [lockouts] are extremely rare, and to the extent they may occur, the unreasonably short reporting deadlines proposed in the [*2016 NPRM*] would do more harm than good.").

III. ANY SENSITIVE, PROPRIETARY INFORMATION REPORTED TO THE FCC SHOULD RECEIVE STRONG CONFIDENTIAL TREATMENT

If the Commission nevertheless adopts false alert or lockout reporting requirements (including the email reporting obligation that it adopted in July), it should accord strong confidential treatment to any proprietary information that may be included in such reports or indirectly revealed through the reporting process.[20] As the Commission observed in its *2016 NPRM*, reports involving company-specific network, equipment, or subscriber information "may contain material that, if disclosed, could potentially cause substantial competitive harm to the EAS Participant or even undermine national defense and public safety."[21] As NCTA explained in 2016, "proprietary details about the operation, security, and vulnerabilities of EAS equipment are highly sensitive and must be protected against disclosure to those who would bring harm to the nation's critical communications infrastructure, as well as from competitors who may seek economic advantage."[22] Despite these important concerns, the *Report and Order* does not address confidential treatment of false alert reports, and the *Further Notice* appears to suggest that such reports might be shared broadly among "affected stakeholders."[23]

At a minimum, the Commission should adopt its tentative conclusion from the *2016 NPRM* that false alert and lockout reports (including any emails sent to the FCC Ops Center)

---

[20] In many cases, EAS Participants may have very little information on a false alert beyond publicly available news reports, as discussed above. But to the extent that an EAS Participant's explanation of the transmission of a false alert includes sensitive, non-public information (e.g., location or configuration of EAS equipment or specific vulnerabilities contributing to the false alert), the Commission should protect that information against public disclosure, as it has in analogous contexts.

[21] *2016 NPRM* ¶ 150.

[22] *NCTA 2016 Reply Comments* at 8.

[23] *Further Notice* ¶ 40. Certain commenters' support for the reporting requirements proposed in 2016 was premised on the expectation that false alert and lockout notifications would be broadly disseminated to state and local governments, public safety answering points ("PSAPs"), and other emergency management authorities in affected jurisdictions. *See* APCO International Comments, PS Docket No. 15-94 at 5-6 (June 8, 2016) (stating that "having timely information about false alerts and equipment 'lockouts' could be very useful to PSAPs and

should be treated as presumptively confidential and not routinely available for public inspection.[24] Such treatment would be consistent with the Commission's well-established presumption of confidentiality for Network Outage Reporting System ("NORS") data,[25] as well as its presumption of confidentiality for "test data and reports containing individual test data" submitted via ETRS.[26] As with ETRS data, the Commission should also condition any sharing of reports with state emergency management agencies on a certification that those agencies have "confidentiality protections in place at least equivalent to those set forth in the federal Freedom of Information Act (FOIA)."[27] As the *2016 NPRM* observed, "it would seem that Part 11 information sharing should be permitted by the Commission only if stringent measures are in place to protect the data from public disclosure."[28]

Therefore, to the extent the Commission proceeds with new reporting requirements, it should provide a strong presumption of confidential treatment for proprietary information and should not risk harm to competition or public safety through broad disclosure to third parties. The Commission should also give due consideration to the competitive and public safety implications of including report data in public documents without appropriate aggregation and

---

other officials in identifying and mitigating problems with the EAS and WEA"); New York City Emergency Management Department Comments, PS Docket No. 15-94 at 10 (June 8, 2016) ("Upon learning of or observing a false EAS activation, the affected EAS Participant(s) should be required to immediately report the alert to the Commission and, more importantly, the state and/or local governments (emergency management offices and/or public safety answering points) for the jurisdictions whose public received the alert."). While NCTA does not doubt these entities' good intentions in seeking access to such information, distribution of false alert or lockout reports to potentially thousands of jurisdictions nationwide would increase exponentially the risk of inadvertent disclosure and compromise EAS Participants' ability to protect their networks against malicious activity, including future false alerts.

[24] *See 2016 NPRM* ¶¶ 146-150 (citing 47 C.F.R. § 0.457).

[25] *See* 47 C.F.R. § 4.2.

[26] *See 2016 NPRM* ¶ 31 n.102.

[27] *See id.* ¶ 153.

[28] *See id*.

anonymization. In no event should EAS Participants or any other EAS stakeholders be required to report sensitive network information to the Commission without knowing whether some or all of that information may later be disclosed to third parties.

IV. STATE EAS PLANS ARE A BETTER APPROACH TO PREVENTING AND CORRECTING FALSE ALERTS

The *Further Notice* proposes "to require State EAS Plans to include procedures to help prevent false alerts, or to swiftly mitigate their consequences should a false alert occur."[29] Such information "could be supplied by state and local emergency management authorities, at their discretion, to SECCs for inclusion in the State EAS Plans they administer, and would then be available to other emergency management authorities within the state for quick and easy reference."[30]

To the extent the Commission takes any further action with respect to false alerts, this approach would address its concerns more directly and be far more likely to lead to meaningful improvements in relevant operating procedures. Emergency managers and alert originators – not cable operators or other EAS Participants – are in the best position to develop and implement procedures to prevent and correct false alerts. Adding such information to State EAS Plans would have the dual benefits of establishing clear roles and responsibilities for all entities involved in alert origination and transmission while also encouraging SECCs to review and update plans already on file. Cable operators welcome the opportunity to participate in SECCs and work with stakeholders in each jurisdiction to educate them about the technical

[29] *Further Notice* ¶ 44.

[30] *Id*.

characteristics of cable systems and develop appropriate training and coordination procedures to mitigate the risk of any future false alerts.

Finally, while the Commission plays an important role in EAS governance, many of the issues identified in the *Hawaii Report* and the *Further Notice* fall more within the purview of FEMA and state and local emergency authorities. In the months following the Hawaii incident, the Commission has made helpful contributions by convening stakeholders, promoting best practices, and encouraging communication and cooperation between alert originators and EAS Participants. These activities can – and should – continue independent of any further action in this proceeding. But the fact that the FCC regulates communications providers does not mean that every challenge in emergency alerting can be solved through increased regulation of EAS Participants. Instead, the Commission should continue to work with its partners in government to more directly address issues within each agency's jurisdiction and expertise.

CONCLUSION

For the reasons discussed above, the Commission should revise the false alert reporting mandate it adopted in July to permit reporting by alert originators, decline to impose any further false alert reporting requirements for EAS Participants, and reject the proposal to require reporting of lockouts. To the extent the Commission requires such reports, it should adopt a strong presumption of confidentiality for proprietary information.

Any further FCC action with respect to false alerts should focus on updates to State EAS Plans to help clarify the roles and responsibilities of all entities involved in alert origination and transmission, not additional regulatory burdens for EAS Participants.

Respectfully submitted,

/s/ Rick Chessen

Rick Chessen
Loretta Polk

NCTA – The Internet & Television Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

Andy Scott
Vice President, Engineering Technology

September 10, 2018