

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

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

COMMENTS OF AT&T

AT&T Services, Inc., on behalf of its affiliates that provide Direct Broadcast Satellite and IP television service (collectively, AT&T), hereby submits these comments in response to the Commission’s Emergency Alert System (EAS) Notice of Proposed Rulemaking.¹ These comments focus on the Commission’s proposals to establish a new annual certification regime related to the network security practices of EAS Participants² and a “lockout” reporting requirement, as well as the Commission’s proposal to extend Wireless Emergency Alert (WEA) requirements to tablets. For reasons we provide below, the Commission should resist the urge to respond to a few isolated incidents that have occurred over the past decade with sweeping annual certifications covering over 27,000 entities. If the Commission ultimately adopts a new certification rule, AT&T recommends that the Commission limit its applicability and tighten the

¹ *Amendment to Part 11 of the Commission’s Rules Regarding the Emergency Alert System, Wireless Emergency Alerts*, PS Docket Nos. 15-94, 15-91, Notice of Proposed Rulemaking, FCC 16-5 (rel. Jan. 29, 2016) (*NPRM*).

² *See* 47 C.F.R. § 11.2(d) (defining EAS Participants as “[e]ntities required under the Commission’s rules to comply with EAS rules, e.g., analog radio and television stations, and wired and wireless cable television systems, DBS, DTV, SDARS, digital cable and DAB, and wireline video systems”).

language of the certification to remove any ambiguity. Similarly, it should reconsider the need for lockout reporting since, based on the Commission's own data, these issues rarely occur. If the Commission adopts a lockout reporting rule, we recommend that reporting entities be provided a sufficient amount of time to file initial and final reports. Finally, we discuss the technical challenges to extending WEA requirements to tablets, as well as some other WEA matters.

Security Certifications. The Commission proposes to require all 27,000+ EAS Participants to file annual officer-level certifications on security matters, which the Commission contends will make the EAS system more secure and reliable.³ As described by the Commission, the impetus for the proposed certification are six isolated events over the past nine years, which the Commission states “demonstrate[s] that there are significant vulnerabilities in the nation’s EAS infrastructure that must be addressed comprehensively.”⁴ AT&T disagrees with that assessment. The incidents that the Commission documents in its *NPRM* show that there is no systemic weakness in the nation’s EAS regime. To the contrary, given the vast number of EAS alerts that are issued each year, the EAS system functions remarkably well, with a high degree of accuracy. Moreover, by adopting its proposal to add a “year” parameter to the time stamp in the EAS protocol,⁵ the Commission will eliminate a known deficiency in the over-the-air EAS system. Perhaps, the most effective approach to addressing the Commission’s EAS security concerns is for the Commission and other governmental entities to expedite the transition from the legacy, over-the-air EAS regime to the Federal Emergency Management

³ *NPRM* at ¶ 111.

⁴ *Id.* at ¶ 97.

⁵ *Id.* at ¶ 141.

Agency-administered Integrated Public Alert and Warning System Open Platform for Emergency Networks, which, by design, is a more secure system.

The few incidents that the Commission describes in the *NPRM* do not appear to implicate the security practices of non-broadcasters, like AT&T. Rather, all of the lapses identified in the *NPRM* appear to involve only radio and television broadcast stations. And, had these stations followed today's industry best practices, it does not appear that downstream, non-broadcasting entities like AT&T would have been affected by any of these issues. The Commission thus has offered no justification for imposing the broad certifications contained in proposed rule 11.44 on non-broadcasting EAS Participants, and should apply any EAS security certification requirement it adopts only to radio and television broadcast stations.

While AT&T believes the proposed certification is unnecessary and should not apply to non-broadcasting EAS Participants, it nonetheless has concerns with aspects of the proposed certifications. First, AT&T recommends that the Commission delete proposed section 11.44(a)(1) in its entirety. Proposed section 11.44(a)(1)(i) is unnecessary, and proposed sections 11.44(a)(1)(ii) and (iii) are vague and also unnecessary. By certifying (or not) to the specific statements contained in proposed section 11.44(b), a responding entity either will or will not have "satisfied the obligations of subsection (b) of this section." Thus, there is no reason to require the duplicative certification in section 11.44(a)(1)(i). The proposed certification in section 11.44(a)(1)(ii) is problematic in that it requires an officer to certify that the company has "adequate internal controls to bring material information regarding network architecture, operations, and maintenance to the Certifying Official's attention." This certification on its face is not tied to EAS participation and, even if it were, it is impossibly vague. No certifier could have any idea what is meant by "material information regarding network architecture" or, for

that matter, “material information regarding . . . operations” or “material information regarding . . . maintenance.” It is unfair to put any company’s employee in the position of having to certify under penalty of perjury to vague and ambiguous statements like those contained in proposed rule 11.44(a)(1)(ii).⁶ Moreover, such certifications are unnecessary. The Commission proposed specific certifications in section 11.44(b) to capture information the Commission has deemed relevant to maintaining a secure EAS system. The Commission has offered no similar explanation for why the additional information in section 11.44(a)(1)(ii) is necessary. Lastly, proposed section 11.44(a)(1)(iii) requires an officer to certify under penalty of perjury that his/her company has made the officer “aware of all material information reasonably necessary to complete the certification.” This is yet another certification that is unfair to the certifier. Rather than requiring someone to certify under penalty of perjury that he/she has been provided “all material information” by others, the Commission should allow companies to follow their standard internal procedures designed to enable company officers to make the substantive certifications set forth in proposed section 11.44(b). This is precisely how companies respond to other Commission-required certifications.

⁶ AT&T understands that the Commission merely copied language from its existing 911 reliability and resiliency certification rules for proposed section 11.44(a)(1). *See* 47 C.F.R. § 12.4(a)(2). However, public safety certifications are not one-size-fits-all. While this language may make sense in the 911 reliability context – though AT&T doubts it does – the Commission has failed to demonstrate why these certifications make sense here. Moreover, we note that the Commission added the definition of “certification,” which contains substantive certification requirements, to its final 911 reliability rules without notice and comment. *See Improving 911 Reliability; Reliability and Continuity of Communications Networks, Including Broadband Technologies*, PS Docket Nos. 13-75, 11-60, Notice of Proposed Rulemaking, 28 FCC Rcd 3414 (2013). Had the Commission sought notice and comment on this proposal in the *Derecho* proceeding, AT&T, and, perhaps others, would have expressed the same concerns raised here. Simply because the Commission requires these unfortunately vague certifications in a different context does not mean the Commission should compound this mistake by extending those same faulty certifications to EAS Participants.

Second, the Commission should define key terms used in proposed section 11.44(b). For example, in section 11.44(b)(1), officers must certify under penalty of perjury that their companies have identified and installed updates and patches to “EAS devices and attached systems” in a timely manner. As currently drafted, “EAS device” is undefined yet an officer must make a certification with respect to the status of such “devices.” The Commission defines “Intermediary Device” in its rules.⁷ Is that the device the Commission intended to cover by the term “EAS device”? If there are other devices, what are they? EAS Encoders, EAS Decoders, Attention Signal generating and receiving equipment? The Commission should provide clarity about which devices and attached “systems” are to be covered before requiring someone to certify compliance as to such devices and attached systems under penalty of perjury.

Third, the Commission proposes to permit covered entities to certify that they have adopted “alternative measures” designed to address the security concerns discussed in the *NPRM* and the proposed rules. AT&T appreciates the flexibility that the Commission is proposing to give to certifying entities; however, absent any guidance on what might be an acceptable alternative measure, this flexibility may not be meaningful. In other words, an officer may be uncomfortable relying on an alternative measure if that company has no idea whether the Commission would agree that the company’s approach is acceptable. In the 911 reliability and resiliency proceeding, the Commission described acceptable alternative measures.⁸ If the Commission adopts some version of its proposed certification rules, AT&T urges the

⁷ See 47 C.F.R. § 11.2(i).

⁸ See generally *Improving 911 Reliability; Reliability and Continuity of Communications Networks, Including Broadband Technologies*, PS Docket Nos. 13-75, 11-60, Report and Order, FCC 13-158 (2013).

Commission likewise to give respondents guidance on acceptable alternatives in its order adopting these rules.

Fourth, the Commission’s proposed rule requiring compliance with “industry best practices”⁹ is vague and unenforceable. As a general matter, the Commission should not adopt rules that cannot be enforced. Tying compliance to generic undefined “industry best practices” is an example of such a rule. Additionally, the Commission should understand that simply because an EAS Participant has established a firewall – an EAS Security best practice¹⁰ – does not guarantee that the firewall will be effective if the Participant also does not enable appropriate filtering or other protection on the firewall, which is something not addressed by the best practice.¹¹ Finally, industry best practices can and do evolve over time. What might be deemed an “industry best practice” today, may not be the following month, when, perhaps, the entity needs to make its annual certification. Is an entity in compliance with this requirement if it is still following the prior industry best practice when it makes its certification? How long should an entity have to get into compliance with the most recent industry best practice? Does that response vary depending on the type of best practice? The Commission and certifiers will have to confront these issues, and many others, if the Commission opts not to base these rules on defined standards and, instead, adopts its “best practices” proposal.

⁹ See, e.g., section 11.44(b)(3)(i)(B).

¹⁰ See CSRIC IV, Working Group 3 Emergency Alert System Initial Report, at 13, May 2014 (“At a minimum, EAS participants should always use a firewall between EAS equipment and the public Internet to reduce unknown external actors from compromising the system.”), available at https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG3-EAS_SECURITY_INITIAL_REPORT_062014.pdf.

¹¹ This best practice also does not address what type of firewall (e.g., packet filtering, stateful inspection, proxy) an EAS Participant should use to secure its EAS equipment.

Lockout Reporting. The Commission proposes to adopt a new rule requiring EAS Participants that experience a so-called “lockout” to submit initial and final reports to the Commission describing that event.¹² As described by the Commission, a lockout generally occurs when video customers’ set top boxes are unable to return to normal operation after an EAS alert, which may result in customers being unable to change their television channels.¹³ AT&T also has concerns with this proposed rule, which it believes is unnecessary because lockouts are so infrequent.

The Commission proposes to require EAS Participants to file an initial report within mere minutes of discovering that its “equipment causes, contributes to, or participates in a lockout that adversely affects the public.” Fifteen minutes simply is an inadequate amount of time for any entity to file a report at the Commission, let alone one that identifies devices affected by the lockout. Lockouts are rare events¹⁴ and if one occurs, affected EAS Participants should spend those first few minutes trying to resolve the lockout, not hastily compiling and submitting some report in order to avoid a penalty for missing the fifteen minute deadline. Instead of the impossibly short fifteen minute proposal, AT&T recommends the Commission provide affected EAS Participants up to 24 hours to file an initial report. This amount of time will ensure that the reporting entity will have prioritized resolving the lockout over submitting reports that may contain incomplete information. Additionally, in the event an EAS Participant learns of a lockout after the fact (*i.e.*, after the lockout has ended), the Commission should clarify that an

¹² See section 11.45(b)(2), (3).

¹³ See *NPRM* at ¶ 132.

¹⁴ See *id.* at n.261 (estimating that there is one lockout per year).

initial report is unnecessary since there would be nothing for the Commission to actively monitor.

The amount of time the Commission proposes for final reports – 72 hours – is likewise unacceptably brief. 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. Finally, it is unclear what information the Commission is seeking when it requests the “mitigation steps taken.” Is the Commission requesting information about what actions the filer took to resolve the reported lockout as quickly as possible or is the Commission seeking information about what steps the filer is taking to reduce the likelihood that such a lockout will recur? AT&T recommends that the Commission clarify its intentions before finalizing this rule.

WEA. Although the Commission has an open rulemaking on revising its WEA rules,¹⁵ it nonetheless requests comment on additional WEA issues in the *NPRM*, including whether the Commission should deem tablets as “mobile devices” for purposes of the Commission’s WEA rules.¹⁶ As an initial matter, AT&T recommends that the Commission take care not to conflate WEA with EAS alerts and/or to extend EAS requirements to the WEA regime. As designed,

¹⁵ *Improving Wireless Emergency Alerts and Community-Initiated Alerting*, PS Docket No. 15-91, Notice of Proposed Rulemaking, FCC 15-154 (2015).

¹⁶ *NPRM* at ¶ 93.

WEA serves as the proverbial “bell ringer” for certain events whereas EAS alerts provide the public with the details about those events. This difference is purposeful and was done because of the technical limitations of commercial mobile service (CMS) providers. We do agree with the Commission that the scope of State EAS Plans should be expanded to include WEA.¹⁷ If the Commission determines that WEA should be included in State EAS Plans, then State Emergency Communications Committees must include CMS representation to ensure that the State Plans reflect accurately WEA capabilities.

The Commission asks whether tablets should be defined to be within the scope of the WEA rules and whether there are any technical impediments to tablets supporting WEA messages.¹⁸ Currently, 4G LTE-enabled tablets do not support the distribution of WEA messages. For that to change, it is our understanding that the industry, working through the Alliance of Telecommunications Industry Solutions (ATIS), would have to update certain standards, including the Mobile Device Behavior Specification and other cell broadcast related standards. Such updates may require twelve months or more to complete. Following the standards development, operating software and equipment manufacturers would need to develop the capability in their devices (including the potential for new hardware and software to receive cell broadcast messages) to process and display WEA messages. This means that a customer will have to purchase a new WEA-enabled tablet in order to view WEA messages. We do not believe customers could view WEA messages on their existing tablets.

¹⁷ *See, e.g., id.* at ¶¶ 42, 55.

¹⁸ *See id.* at ¶ 93.

Finally, the Commission seeks comment on a number of accessibility topics related to WEA messages, including machine-generated translation of alerts.¹⁹ AT&T addressed many of these issues in comments it filed five months ago in the *WEA NPRM* proceeding.²⁰ We do not repeat those comments here but we urge the Commission to consider the significant practical issues identified by AT&T and others with relying on machine translations for WEA messages.

* * * *

AT&T requests that the Commission adopt revised EAS rules consistent with AT&T's comments provided above.

Respectfully Submitted,

/s/ Cathy Carpino
Cathy Carpino
Christopher Heimann
Gary L. Phillips
David Lawson

AT&T Services, Inc.
1120 20th Street NW
Suite 1000
Washington, D.C. 20036
(202) 457-3046 – phone
(202) 457-3073 – facsimile

Its Attorneys

June 8, 2016

¹⁹ *See, e.g., id.* at ¶ 96.

²⁰ AT&T Comments, PS Docket No. 15-91 (filed Jan. 13, 2016).