July 3, 2018

Via FCC Electronic Comment Filing System

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street SW, Room TW-A325
Washington, DC 20554

Re: Preventing False Emergency Alerts and Improving Alert Testing (FCC-CIRC1807-04)

Dear Marlene H. Dortch:
I would like to comment on Notice of Proposed Rulemaking (FCC-CIRC1807-04) regarding the proposed "Preventing False Emergency Alerts and Improving Alert Testing."

If you have any questions concerning these comments, please do not hesitate to call (703-892-1810) or email (sean@donelan.com) me.

Respectfully submitted,

Sean Donelan

1. Errata and Technical Corrections

A reminder, the Commission has not corrected printing and technical errors in Part 11 accidently introduced while publishing past rulemakings:

> § 11.31(c) Since 2012, the second repetition of the example EAS header contains a lowercase "p" between "TTTT" and "JJJHHMM" instead of a hyphen "-". All three repetitions of the EAS header should be identical.
>
> § 11.31(f) Since 2003, the table of State, Territory and Offshore ANSI number codes (SS) repeats ANSI number "68" (Republic of the Marshall Islands - MH) and omits ANSI number "69" (Commonwealth of the Northern Mariana Islands - MP). Then the duplicate code "68" was removed, thus the Commonwealth of the Northern Mariana Islands – MP has been omitted from the table entirely. The table should include each State, Territory and District of Columbia code along with the National Weather Service marine areas once, and only once. Or incorporate by reference the ANSI, Census and National Weather Service geographic code definitions.

2. Lack of Reporting of Public Alert Testing Problems

Testing of the Emergency Alert System and Wireless Emergency Alert system is critical and requires oversight.

In footnote 32, the Commission asserts it has received no complaints that the public was caught unaware by any live code tests. However, the Commission only passively waits for reports. The public often doesn't know to whom to address complaints, so instead they complain to local newspapers and on social media instead of the Commission. If the Commission didn't actively search for EAS problems, it will likely never find any problems and proceed with false confidence.

Just one example, found with a simple Google search:

September 1, 2016: TEMA director apologizes for emergency alert problems

> "The head of the Tennessee Emergency Management Agency apologized Thursday after emergency alerts were sent to mobile devices across the state as a part of a test."
>
> "TEMA heard from hundreds of Tennesseans about problems receiving the messages as well as the confusion and concern they caused, said TEMA Director Patrick Sheehan, in a statement. The Thursday morning alerts were timed with the start of National Preparedness Month and were meant to have limited impact on people."

https://www.tennessean.com/story/news/2016/09/01/tema-director-apologizes-emergency-alert-problems/89723932/

It's understandable the Commission does not want responsibility for pre-approving live-code tests. However, if there is no reporting by the live-code test originator (usually a government agency, such as the National Weather Service or local emergency management agency) about success or problems found as part of live-code testing to the Commission, the Commission may never know that a live-code test occurred. At best, the Commission might only learn about

problems through ad hoc news reports. Not reporting live-code testing results may be good for plausible deniability, but not as good for evidence-based decisions.

3. Piecemeal Compliance Deadlines Increase Costs

Historically the Commission allowed EAS participants to implement EAS upgrades voluntarily and only required when they replaced their EAS hardware. This allowed EAS participants to consolidate several compliance changes with their natural EAS equipment replacement life cycle. The Commission even permitted the addition of CAP intermediate devices with existing EAS hardware instead of replacing existing EAS hardware.

Spreading software changes across different deadlines ends up increasing costs, requiring multiple testing and upgrade cycles at random times of the year depending on unpredictable publication in the Federal Register. Minor changes with multiple different compliance deadlines are often more expensive compared to testing and integrating major changes with a single compliance deadline. Piecemeal software upgrades to meet compliance requirements also provide a justification for EAS manufacturers to charge for software maintenance and upgrade releases.

Footnote 85 indicates that 93.2% of EAS Participants use manufacturer supported EAS equipment which include authentication and validation measures or could be easily upgraded with a downloadable software update. The most critical participants for alert authentication and validation are EAS Participants acting as State and Local Primary Participants. They are also the most likely using newer and supported EAS equipment. The approximate 1,000 EAS Participants (6.8%) still using End of Life or unsupported EAS equipment are likely very small broadcasters and cable systems without the financial ability to upgrade. Fortunately, for alert authentication and validation, those still using EOL/unsupported EAS equipment probably have very little affect on the dissemination of emergency alerts or the presidential message.

The Commission can allow enforcement discretion and grant waivers for small EAS participants without the financial ability to replace operational, but end of life, EAS equipment. It would be cleaner for the Commission to follow its historical practice of allowing EAS participants to voluntarily implement upgrades; and mandate only new or replacement EAS equipment meet new compliance requirements. Critical EAS participants normally implement voluntary upgrades as part of their engineering life-cycle anyway.