RE: FCC FCC-10-11, EB 04-296 , 2nd FNPRM on EAS Review

1. The following comments are submitted by Michael G. McCarthy privately and personally. They do not reflect opinions of his employer or of his clients. Mssr. McCarthy is a professional broadcast engineer certified by the Society of Broadcast Engineers (SBE) as a Senior Radio Broadcast Engineer and Audio Engineer. Mssr. McCarthy is also a member of IEEE and has 34 years hands-on experience in all aspects of radio broadcasting. He is also a licensed radio amateur of 28 years and has spent the same amount of time in all areas of emergency radio communications with regards to local area communications. The comments contained herein pertain exclusively to issues and concerns with regards to Next Generation EAS as defined in Section C of the instant matter.
2. The proposed implementation and dissemination plan of CAP/EAS-II is not the utopic panacea its proponents believe. Actually, many ground level folks charged with implementing CAP/EAS-II in broadcast and cable operations carry grave concerns regarding IP message relay and retrieval robustness. Especially under depleted, damaged, stressed and/or high traffic conditions prior to, during, and after a major event. The bottleneck in communications in Haiti following the earthquake earlier this year pointedly reminds us terrestrial (wire/fiber) schemes are subject to immediate physical disconnection as well as congestion/overloading of remaining facilities. For a period of time, the only transmissions in and out of the island country were by amateur and satellite voice and IP communications. WIRELESS communications.

3. CAP's reliance on the public and station/facility wired IP infrastructure is fraught with fragile and unrecoverable weak links. These weak links are typically not hardened, are not in multi-level federal and state PSAP's and EOCs, their backbone systems, and principal service providers. The weak links are instead the wire "last mile" serving every customer, the wired long distance relays between CO's and their regional hubs, and the station equipment surrounding EAS-II/CAP's equipment.

4. The local carrier's service facilities to the end user, AND the station's IP infrastructure ARE collectively the weakest links with each being a weak link in their own way. This means any station, my station, the guy next store, the city center high rise fed by a Bell Operating Compnay (BOC). And then there is the all too common radio station out on the forgotten rural road served by 40 year old copper through 100 aged and infested splice pedestals. I state this as a factual condition as many of these facilities are served by aging and poorly maintained copper infrastructure left over from the old "Ma Bell" era and

their visionary deployment of copper to all parts of the USA urban and rural. In many operations, that weakest link is exhibited by an end user (least cost) DSL or T-1 circuit riding a conventional BOC 40 year old last mile POTS copper pair fed from an underground service expansion terminal. These facilities are easily crippled by an extended power failure, lightning strike, or flash flood. They are also easily subjected to accidental interruption during maintenance windows, disruption due to excavation, traffic collisions, weather, natural phenomena and/or willful criminal activity. LP-1 and LP-2 station's DSL and T-1 circuits are commonly fed by this method of circuit expansion.

5. A station (or it's internet service provider) with it's phone lines "cut" due to a flood, tornado, hurricane, derailment, accident, or other impact is absolutely and utterly useless to any EMA agency seeking to disseminate a Shelter In Place alert, evacuation orders, other call to action, or status message during or following an event. They're islanded. Even 802.11a serviced stations are not immune from outages as their ISP is likely on terrestrial connection by fiber or copper or the ISP's hardware is similarly not hardened against a like kind failure.

6. Still others do not have IP access at their control points as those locations might be at an unmanned transmitter which is serviced by a simple wireless phone extender for remote control. LP's are received over the air. Further, there are locations in rural towns which are not yet serviced by ANY broadband facilities. They're constrained to bandwidth limited dial-up modems…if that.

7. My specific concern lies in HOW the EAS-II Common Altering Protocol messages will be RELIABLY distributed to the stations and avoid the overwhelmed public IP infrastructure. This presumes the station's wire IP connections remain intact and functioning. This is of paramount concern and it appears those unfamiliar with hardening facilities believe wireline IP access will always be there. Let me again refer to Haiti as superbly splendid example of that false hope and how that will prove otherwise. Wired IP is not a survivable distribution mode in that type of emergency. EXCEPT by wireless means, no IP is possible.

8. There is also a great deal of apprehension regarding the absolute commitment to an IP based system where unstable or hackable operating systems and hardware underpin CAP's dissemination model. Most broadcast facilities operate various forms of Windows and supporting Server configurations sans virus protection in their operations area. Few stations employ virus protection on their audio delivery subnets due to the resources consumed by the now otherwise necessary programs. Most of the time

spent on maintaining involve resolution of viri or machine lock-ups due to some corrupt .INI file, software bug, or misplaced bit during a short fuse power event. Any one of which can cripple a network until a technician arrives to repair/reset the fault. A crippled network also means no IP access. Which means no CAP message capture and dissemination is possible by that station, be it a LP-1, LP-2, or Participating Station.

9. Then comes the various hardware failures too numerous to mention BEFORE maintaining firewalls, routers, and insuring the ports used for CAP are otherwise secured from backdoor hackers. While I believe CAP devices will be secure, it's everything surrounding CAP which typically isn't and will create problems in managing CAP and message dissemination when really needed. In so far as the hardware goes, 99% of all computing hardware is least cost based. Not MIL-SPEC or designed to operate or recover in less than ideal conditions. When the going gets tough, most computing equipment becomes a door stop and IP based station infrastructure will cease to operate leaving largely inexperienced operators to operate the stations in a crisis lacking all previously available resources. All it takes is one good power surge or cup of flood water into a router or switch to bring a station or cluster to it's knees, islanding it from the outside world. The worst result is a crippled router or server when need of IP is the greatest. Without DNS and DHCP provided by a failed/shut-down server, how will CAP equipment navigate to the outside world? Such as when seeking the voice recording of a disseminated message.

10. Finally, there is the concern about traffic congestion. Since only a handful of stations or relay points have high priority QoS traffic routing arrangements with their providers, station originated requests for CAP content will be handled like any other nominal web traffic through the various core providers and networks. And as what happens with telco during periods of heavy demand, there will be blocks, delays and/or timeouts when asking for data from overwhelmed circuits, routers, and servers all through the web. That is, of course, presuming they don't crash or are otherwise impaired beforehand, including a coordinated DOS attack by a national enemy. I see this potentially happening with any national coordinated test.

11. On a wide scale emergency, where will all the bandwidth, distribution, and routing capacity come from to support and insure CAP message dissemination. How will the so called "priority" requests from devices seeking to download large file audio messages be handled in that moment of incredible peak demand? Who will repair that pipeline when it breaks down?

12. While this may sound backward thinking, automated delivery of the voice file by a radio method sounds plausible. The present SAME system of preamble and EOM seems to work at the most basic level. This is the method used by the State of Illinois to distribute their monthly test. Granted, there are issues with audio quality and such which make the audio quality less than desirable, those issues are easily corrected and even hardened in a digital network where analog noise is no longer an issue. In this mode (and the same mode used by other states to largely the same degree) UDP is used and external IP connectivity is a side-stepped issue.

13. While there is talk of satellite delivery, it's a ways off for many states. Plus satellite too is fraught with many weak link and delivery issues. A solution to this pradox is the SBE's proposal for a number of narrowband channels in the freshly re-allocated 700mhz bandplan. It is currently in stasis and I strongly suggest that proposal should be considered for any national, state, regional, and/or local distribution plans. I can not think of a better utilization for those channels than true inter-agency and inter-industry operatibility linking for emergency commincations.

14. But this fact remains true with any RADIO distribution system: State and local agencies can control the distribution medium to the LP relays/stations on their PRIVATE RADIO networks as could be constructed per the SBE's proposal. Not through failure prone telephone circuits, public web, nor least-cost station computing equipment. Nor via the public web one request at a time no matter the speed of the router and switches. UDP delivery of a voice and/or data file can be distributed by radio direct to the EAS device and thus would avoid/sidestep the whole public web and public switched phone network. And if done correctly, private radio network message delivery direct to the CAP device completely bypasses the station's vulnerable wired and wireless IP infrastructure as well. Thus insuring the message gets through when the local conditions are difficult or catastrophic and the CAP equipped facility is otherwise isolated or islanded.

15. The bottom line is simple: Aside from the fact CAP compliant EAS-II is an unfunded mandate imposed on the stakes holders, message dissemination, access and retrieval by the public web and station IP infrastructure is a distribution linking system predisposed to fail in any type of local, regional, or national crisis. Broadcasting is a RADIO medium. EMA is a RADIO centric operation. RADIO systems can be hardened quite effectively. Unlike wired IP, RADIO (analog or UPD) survives catastrophic events with little remedial attention if the infrastructure is so hardened. We should be using RADIO to it's maximum capacity for distribution. HF, VHF, UHF. It doesn't matter which spectrum is used as long as the service

satisfies the technical requirements and IS THERE WHEN NEEDED. Less we concede one more thing to wired IP just because we find wired IP to be an expedient convenience…never minding it's countless failure modes and weak links before we even consider traffic/congestion and service provisions.