Trilithic Inc.

Response to **EB Docket No. 04-296**

In response to III.E.24. and III.E.25.

We strongly recommend that the specific EAS Event code to be used for the National test is identified in the regulations, and suggest the removal of discretionary language such as "or such other EAS codes as the agencies conducting the test deem appropriate". State EAS Plans should be modified to include enabling the test Event. This can only be done if the Event code is identified up-front just as with the EAN and EAT. In addition, having a known, standard code will allow Encoder/Decoder manufacturers to warn EAS participants (through the Encoder/Decoder user interface) if they attempt to disable the test Event. Also, knowing the Event code to be used at the time of sale or firmware upgrade allows manufacturers to educate their customer base in regard to configuring their EAS units. Procedurally, a National test Event should closely mimic an EAN Event, enabled once and kept enabled because it is known to be the national test code.

Since propagation and distribution of the EAN message is key to it's effective operation, the EAS Protocol Text of the test message, with the exception of the EEE (Event), JJJHHMM (Origination Time), and LLLLLLLL (Station ID) should be identical to the protocol text created during an EAN. Since the other fields of the EAS Protocol Text are used in the decision making process for activation, varying other fields of the message may result in a test that does not accurately reflect the success of the EAN distribution.

Since the EAN and EAT codes are unique in their implementation, the specific presentation (visual and audible appearance) when the message is retransmitted can not be tested using any other Event code. This discrepancy between the test and the actual EAN may be acceptable given the highly disruptive nature of the EAN. We believe that the use of another, specific Event code (such as the NPT) is sufficient to test the dissemination of the National message, though not sufficient to test it's presentation, provided the protocol fields of the test message closely resemble those of the EAN.

In response to III.E.29. and III.E.30.

National security should be considered prior to making test data publicly available. Such data may provide information on vulnerable entry points and distribution paths which could be exploited to the detriment of the United States. The specific information listed would reveal the EAS distribution architecture for the entire nation. If this reporting carries over to "next generation" distribution of emergency messages, the information could reveal other, network based distribution architectures.

Data regarding messages received from each source is vital for verification of redundant distribution paths and should be included as anticipated by the Commission. This information is likely to be vital when next-generation delivery systems are on-line. The potential exists for the current FSK audio to (almost) always be detected as a duplicate, and therefore easily ignored until a real emergency situation requires it.

In response to III.E.32.

Encoder/Decoder filtering of the EAN Event for FIPS (location) codes, as well as Originator codes and message expiration (due to clock drift on a seldom used originating system), as prescribed by Commission rules can certainly prevent distribution of the EAN message, or any other EAS message. Failure to test for these fields can result in ease of spoofing, and (in regard to the time and duration) accidental activation by replaying the message (such as in a news report).

In order for the EAN (and EAT) to operate, either Commission rules, or EAN origination and distribution must be modified to match the other; or the behavior of Encoder/Decoders must be modified to intentionally circumvent Commission rules. Current Commission rules do not provide special case filtering exemptions for the EAN and prohibit the addition of codes not sanctioned by the Commission (§ 11.31(c)). Commission rules could be modified to exclude the EAN and EAT from validity checking (in the areas mentioned). Alternatively the designation of a National PSSCCC (location) code could be adopted and used by originators of the EAN Event.

We recommend the addition of a National location code as this allows operation of the Encoder/Decoder in a manner fully consistent with current Commission rules, and is a natural extension of the current EAS protocol. In addition, the code 000000, if used, is currently accepted by multiple "Digital EAS" protocols. Such a modification still requires that the EAN Originators modify their equipment to incorporate a new "FIPS" code and use a valid Originator code. Note that in the February 2002 Report and Order (FCC-02-64) the addition of a National FIPS code "so that multiple alerts are not needed to activate the entire country" was discussed. The reasons for rejecting the addition may still be valid.

From our perspective, if the Commission makes changes effecting the operation of the Encoder/Decoder, the impact is minimal provided a reasonable amount of time is given to enact the change in firmware. Firmware can be distributed over the Internet and no hardware changes are necessary.