Memorandum for: FCC

Subject: Comments on Proposal for Rulemaking RM-11699

1. The proposal for rulemaking, RM-11699, should not be accepted. Encryption of Amateur Radio transmissions will not solve the interoperability issue or the privacy of communications issues raised in the filing.
    a. Interoperability between First Responders and Amateur Radio Operators assisting during an emergency is critical and one of the main functions of Amateur Radio when responding to a disaster. Amateur Radio provides, through its onsite operators, a means to augment emergency communications capabilities and provides an interoperable path for communications between responding agencies. In many cases, this is the only way some agencies can keep in touch and pass message traffic due to incompatible communications systems. If encrypted communications are introduced, yet another "closed link" will exist between two points that fails to allow this interoperability and will prevent everyone with a need to know to remain informed as to what is going on and also keeps affected agencies that are not privy to the communicated information in the dark.
    b. Two means already exist to provide "private" radio communications links between two elements supporting a disaster.
        i. If an agency anticipates a need for an Amateur Radio Operator at a given location will need to pass to them confidential or "classified" information, that agency can simply provide that operator an agency radio that has the appropriate encryption key, operates on the appropriate frequency and uses the same radio transmission protocols.
        ii. The existing 1.25 Meter band allocation for Amateur Radio can be utilized to pass traffic considered confidential. Most scanners do not support scanning the 1.25 Meter Band given that his band is limited to North America. Simply setting up a normal Amateur Radio net on frequencies allocated would provide a high degree of confidentiality in the event that sensitive traffic needed to be passed.
    c. Encryption on Amateur Radio frequencies is not supportable from a technical perspective. Given the technical certifications and capabilities of Commercial vs Amateur radio equipment, encryption will require the Amateur Radio Operator have a personally owned commercial radio capable of encryption. Given the many different manufacturers of commercial radios, the different protocols used (P25, TETRA, etc.) and the different banding of different models of radios, an Amateur Radio Operator would need the same radio type and model as the supported agency in his or her possession prior to the emergency. That radio would need to be programmed on the appropriate agency frequency and it would have to have the current agency encryption key loaded. In an emergency this would dramatically limit the ability of an Amateur Radio Operator to "join" an encrypted radio net run by a given agency. Additionally, if the latter criteria

could be achieved, the Amateur Radio Operator owning the Part 90 certified, programmed and keyed radio could listen to all agency communications during non-emergencies. This could be problematic for some first responders who deliberately encrypt transmissions to limit access to their radio traffic.

2. There are appropriate work-arounds for the problem of passing sensitive radio messages available today without resorting to encryption of Amateur Radio Traffic. The first is for the agency to provide a radio to appropriate Amateur Radio personnel on an as needed basis and taking the radio back once the emergency is past. The second method would be to utilize the 1.25 Meter Band frequencies for sensitive radio traffic. Both methods would work much better, be more reliable and provide better service than allowing encryption on Amateur Radio frequencies.

Respectfully,

Bart Hill

Bart Hill

K7LTC