

As a former communicator in the United States Army, I am familiar with secure communications. The Amateur Service lacks the infrastructure to maintain encryption. Secure systems are complicated to maintain, much more complicated than clear-text (or clear-voice) systems. Because the Amateur Service by its nature lacks direct controls - from an agency such as FEMA or DHS - maintaining a secure network is not plausible. The argument might be made that the Amateur Service has already displayed the ability to deal with a certain amount of security, vis a vis the Volunteer Examiner system, but this is by no means equivalent. Keeping a license-exam answer key from prying eyes is a far, far less challenging concept than keeping secure an encryption system which is designed to keep secure personal information.

The Amateur Service lacks the means to control a secure system. Equipment must be secured at all times, accounted for, maintained, and emplaced for deployment. Individual equipment cannot satisfy this requirement. The attractive benefit of the Amateur Service to a served agency is that the volunteer assistance comes "no-cost" - not only do they not have to pay the operators, but the operators bring their own equipment.

Here in the US Virgin Islands, Amateur Service licensees play a large role in emergency communications. The VI Territorial Emergency Management Agency (VITEMA) considers us a critical part of the Territory's emergency plan. In times of crisis here, licensees of the Amateur Service in the Territory have made invaluable contributions using conventional analog systems and modes which have been used in such fashion for years, which have achieved commonality in the Amateur emergency-communications community, and which are readily available to Amateur Service licensees. There is no pressing need to complicate this excellent, functional, extant situation to vaguely attempt to accommodate a requirement which may or may not actually become relevant, here or elsewhere in the FCC's jurisdiction. Should it become relevant, existing Part 15 licensees can provide encrypted wireless information transfer without changing the Part 97 rules, and Part 15 is a more appropriate venue for encrypted traffic.

From an international-relations standard, encryption is at best counter-productive and at worst actually destructive to Amateur Radio's traditional role as technical ambassadors. Foreign governments see Amateur Radio as harmless, technical hobbyists who communicate with each other about topics of mutual interest. They know they can easily monitor Amateur transmissions to ensure the hobby of Amateur Radio does not conflict with what that government may see as a security interest.

Finally, encryption defeats the self-policing nature of the Amateur Service. The FCC has enough enforcement work. Does the FCC really wish to take on the additional workload of attempting to enforce Amateur Service encrypted signals?

I urge the Commission in the strongest possible terms to deny encryption in the Amateur Service.

Regards,  
Robert Davis  
Amateur Service Callsign WP2XX