

As a Network Security Architect for a major financial institution, and as a amateur Radio operator with a general license (K7ABB) I do have an interest and understanding of the issues surrounding the use of encryption in high speed wireless networking utilizing amateur radio equipment. With that knowledge and interest I support the Petition of Don Rolph to clarify and allow the use of encryption on amateur assigned frequencies, especially as it relates to networks using high speed broadband mesh capability in support of emergency communication activities. My support is however, tempered with some reservations that will need to be addressed in the final rule making.

I do understand that the use of encryption can have significant impact in areas of enforcement and the potential misuse of encryption to hide the content of messages from regulators, law enforcement, and in cases where the radio signal crosses international boundaries there could be an impact to treaties and national security. As the FCC addresses the question of allowing the use of encryption I do recognize that they must remain aware of these overriding issues and the potential for abuse that encryption might present if implemented.

It is well known that in cases of disasters the normally established telecommunications systems are either damaged, overwhelmed or both forcing emergency responders to seek alternative means of communications. Amateur radio service has been frequently called upon to fill that requirement for an alternative communication medium. As Technology improves the abilities of the amateur to provide high speed multimedia communications options are also improving.

As mentioned in Mr Rolph's petition there are instances in the support of emergency communications where an amateur may be called upon to transmit messages containing various types of protected information. Three such examples include health information protected by HIPAA, Personal identifiable Information (PII) that could expose victims to fraud, and information that could provide insight into ongoing criminal investigations. Amateurs should be allowed to take reasonable measures to protect the content of any information that potentially falls into some protected category.

It should also be recognized by the FCC that encryption is no longer viewed solely as a means of keeping information secret. It has also evolved into a method of protecting networks from harmful interference by limiting the participants to those who have knowledge of the keys, certificates or cyphers that enable the encryption. This aids in maintaining message integrity and in the integrity of the network involved.

The definition of harmful interference can, and should, include hacking and cyber attacks on a shared medium network such as the recently formed HSMM-Mesh, also known as Broadband-Hamnet. This particular network utilizes consumer grade hardware and radios on frequencies in the 2.4Ghz range that are shared by Amateurs and consumers alike. Because several of the channels in this frequency range are shared it is possible for harmful players to attempt to interfere with that network, and would be very successful if some precautions were not taken. The consumer equipment is already capable of encryption for the specific purpose of limiting the risk of hacking and misuse of the available networks.

The goal of the FCC in this case should be to find a reasonable balance between the needs of emergency and protected information flow, and the precautions that need to be taken to prevent abuse or illegal activities that could be hidden within the encrypted information flow. To find this balance I would add to

Mr Rolph's petition a better definition of "messages encoded for the purpose of obscuring their meaning" to include acceptable and unacceptable uses of encoding messages.

I would also encourage the FCC to require that any encryption be limited to methods that utilize pre-shared keys, certificates or cyphers so that recordings of the encrypted data could be later unencrypted and reviewed. The FCC should also require that the cyphers, keys and certificates be maintained in a log by the operator, and if possible they should also escrow copies of that encryption material with a third party. That third party could even be a registry provided by a government agency for easy retrieval and inspection. The encryption material must be made available by the operator(s) to be inspected by the FCC, and or any authorized government agency.

I believe that if amateurs provide such encryption material that permits the FCC and other agencies to decode the material after the fact, they would provide regulators a means to verifying the content and assuring that the traffic does not violate the intended purpose of the original rules, while still allowing for appropriate protection of data that may fall into some protected category of sensitivity.