

## James L. (Larry) Randall

5709 Kettering Court, Richardson, Texas, 75082

Tel: 214-536-0325 · [Larry@NREGroup.net](mailto:Larry@NREGroup.net)

28 June 2013

Federal Communications Commission  
Washington, DC

RE: RM-11699

Honorable Members of the Commission:

I am a former Senior Field Engineer and Product Concept and Development Engineer for one of the three top cryptographic companies in the world. As such, I have experience with Diplomatic, Strategic, Tactical, and Privacy levels of encryption over HF, VHF, UHF, SATCOM, and cellular radios, as well as landline and terrestrial microwave. I am also a former FCC First Class Commercial Radiotelephone License holder, a current General Radiotelephone (lifetime) license holder, and an Extra Class Amateur Radio License holder first licensed over 51 years ago.

I have been an Emergency Management volunteer for The State of Texas, Dallas County Texas, Collin County Texas, and City of Richardson Texas for over 25 years. I deployed to Bogalusa, Louisiana as a communicator supporting Baptist Men Feeding and Chain Saw Units from Texas and five other states, and the American Red Cross. I was the State of Texas liaison for two cities following tornado strikes, and handled the initial requests for assistance from the cities to the state. Finally, my articles “*An Illusion of Secrecy*” (about Public Safety encryption) and “*Real World Disaster Communications – Planning for the Unforeseeable*” were serialized by *Public Safety Communications Magazine*.

I submit that my background and experience uniquely qualifies me to assess and comment upon the proposed rule.

In general, I see no reason to modify the rule to blanket permit encryption. I do, however, think it is appropriate to provide for reasonable and necessary accommodation to allow encryption on a **proof-of-need** basis. The served agency should bear the requirement to prove need, and should manage the keys.

In many years, I have not seen a case where lack of encryption capability actually limited my ability to communicate needed information in a disaster response or recovery scenario. Victim names and HIPAA protected information rarely need to be communicated – *but there is that pesky word “rarely”*. My personal operational mindset under current rules is that the communicator and the medical professional at the scene must decide if transmission of protected information in clear is justified to save a life / lives. If so, transmit it, and deal with any consequences later. *Obviously, this is not a comfortable choice, and carries risks for the communicator, for the medical professional, and possibly for other entities.*

I suggest that firmly established ground rules be established to allow encryption ONLY of information that is either medically protected (i.e., HIPAA) or deemed to be a security or safety issue (including avoidance of panic). The FCC must have immediate access to the encryption keys, must be immediately notified of use (or as soon as possible, for the case of communications outage with no outside area capability). In an ideal world, an FCC Waiver would be granted prior to use – but a requirement for that would establish a criterion for something that simply is not possible in many disasters.

Others have discussed issues with key management. I see no such issues. There are many pen and paper ciphers that would provide Privacy to low Tactical security, and at least one that would provide Strategic level security – all at zero cost. Any of these could be adapted to software – but I emphasize that ONLY the protected information must be enciphered. This means that a message could say “YUVKS ODGTH WAGTK HWQPX ZKORQ are being transported to ZKIRJ OVRWQ. ETA 20 min.”. Please note that this message may be transmitted either by voice or by any digital method.

Because the served agency(ies) must be responsible, **under FCC guidance**, for the keys, I suggest that the FCC allow local jurisdictions to choose the cipher along these lines. PRIVACY/LOW TACTICAL: A progressive alphabet mono-alphabetic substitution provides reasonable break resistance, while a five character code group arrangement eliminates clues to the length of individual words – making entry much more difficult. STRATEGIC: The One Time Pad is both theoretically and practically unbreakable. Discs or pads of these should be kept under lock at hospitals, EOC, and other areas where sensitive information may be transmitted or received. The index to be used may be transmitted in clear, so that all parties may be instantly synchronized. Each message must use a different key – therefore each message would have a different index.

Commercial and open source encryption programs such as RSA and PGP are not suitable for these reasons: 1) Message expansion – The encrypted message would be several times longer and would take much longer to transmit; 2) error expansion – a single dropped or wrong bit could render the message unreadable, requiring error correction, further extending time-on-air, and making point-to-multipoint communication difficult to impossible; 3) portions of the message cannot be in clear, as it is “all or nothing” encryption; and 4) the resulting message cannot be transmitted by voice.

I would encourage that the Commission require that any encryption system to be used accommodate both voice and digital transmission. In many cases, voice equipment is available but digital facilities are not. Any system intended for use in a disaster must be biased toward the principle of simplicity of operation. In a radio environment, this means that we must assume that only voice communications will be immediately available – but we must also design for the seamless introduction of digital communications as a replacement or as an additional channel.

I will be happy to respond to any questions that the Commission may have, and will volunteer time to assist with encryption system design and/or selection.

Respectfully,



James L. (Larry) Randall  
WA5BEN  
PG-10-5428

Pro Se