

FirstNet Threatens Cyber Security to State Opt-Outs? DR MICHAEL MYERS

Have you read some of the latest on FirstNet? The most recent article on Urgent Communications about securing FirstNet and the Opt-Out States was a statement by Mike Poth, CEO of FirstNet, caught my eye.

"We have been very vocal that we are going to be unrelenting and unforgiving in our approach to an examination of cyber for states as they consider alternative courses," FirstNet CEO Mike Poth said.

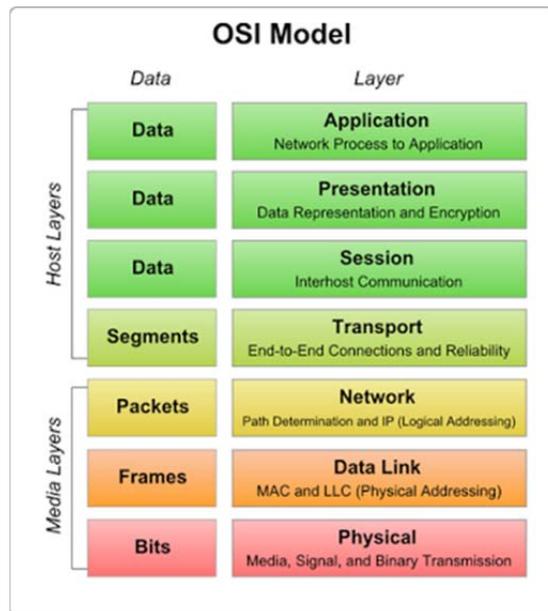
I'm not sure how to read this – is it a threat or an internal view of how they will approach their own philosophy of deployment? Why would a centralized big federal organization believe it can do cyber security better than a small nimble and isolated State? The biggest contributor to cyber security issues is blanket, centralized, connectivity. The biggest detractor to cyber security issues is the isolated and un-centralized network. Why you ask, well because the big-centralized-network is a much bigger target and will obviously have many more opportunities of penetration. Why target a single State network if I can take out the entire eastern region of the United States? Plus, why would a centralized federal government agency feel it can better manage the local cyber security needs of a State?

Regardless, what Mr. Poth is failing to realize, cyber security is a multilayered issue not one size fits all. The State and the centralized federal oversight solutions will all have cyber security requirements. There are many holes to plug the bigger the network gets, but the best approach to securing the infrastructure is the opposite of centralization – a balanced decentralization. Take for example voting machines: the best approach to online voting machines are isolated and decentralized voting machines that insure an inherent quality of unstandardized technologies. If you centralize all the voting machines under one form of technology -- under one controlling entity like the federal government – then the risk of exploitation is much greater. Why? Because its less the Blackhat has to target to make the biggest impact. Through decentralization the Blackhat can't influence the whole enchilada only an isolated island of information, plus it takes a lot of resources to target such a small target that will ultimately have a limited impact.

So why would Mr. Poth threaten a State with *"unrelenting and unforgiving in our approach to an examination"*? I would think the opposite may actually be true, whereas the State will hold FirstNet to the fire on securing the network from the national layer. Then again no one will ever be held truly responsible for any penetration, but if someone is to be held to a standard, I can guarantee you it won't be the State. I'm hoping that what Mr. Poth meant was that they can be trusted that they will address cyber security as a real requirement for the entire network and that the State can trust in them to ensure that, at least, the federal layer will "be secure". If I'm a Governor of a State I wouldn't trust anybody with securing my network, especially those that sit in an office a thousand miles away. I would only trust in those I can control locally. It's much easier for my IT guy to go down to our datacenter and pull a cable to stop a DDOS attack than to call someone in DC to do the same. I know that's over simplified, but the analogy is solid.

Securing the network is the main reason I state that the National Public Safety Broadband Network is not a network, but rather a physical infrastructure. Securing the infrastructure is where cyber security needs to start. Sharing a network architecture with a commercial carrier, who will use it for their own needs first, will not secure the infrastructure. In fact, a commercial carrier partner will make it less secure.

Trying to explain the need to secure a telecom/broadband network to the leadership within the federal government is futile. But, I will give it a try. A long time ago in a galaxy far-far-away we had what's called the OSI Stack – Open Systems Interconnect Stack.



Securing any network infrastructure has to start at the bottom of this stack and then move upwards. The cornerstone to securing any of the networks we have today starts at the Physical layer. The physical layer is where we physically have cables, electronics, facilities, etc... Anything that is “Physically” there, that could be conduits, cables, racks, doors, fiber, trays, etc... Unfortunately, Mr. Poth, thus FirstNet, does not understand that you can’t secure the physical layer in Kentucky from an office in DC – locally control is the only way.

Following the Physical layer, we move into the actual Data Link and the Network layers. The Transport layer can be in this mix as well because much of the data and networking traffic is “transported” in protected virtual channels insuring path determination through IP planning, i.e. Ethernet Optical Transport or Fiber Channel type requirements. Securing the Data Link and the Network layers is typically a function of packetized address, i.e. you physically deny or allow certain IP or MAC addresses onto your local network. You can also isolate transport protocols as well, such as Dense Wave Division Multiplexing or DWDW, or even isolated Lambda connections, i.e. different colors of the spectrum within a fiber. As you can see we can have many tangents of protection that can start within layers 1-4. You can isolate networks, clients and users at all 4 layers, then it really starts to get interesting.

The Session, Presentation and Application layers are where the real paths happen. First we isolate data traffic in multi-layers through the physical, data link, network and transport layers, i.e. for a single user I can isolate his traffic on his own fiber, within his own lamda, isolating on his own spectrum, using his own MAC or IP pool, then wrap it within a Virtual Private Network. Now with the Session, Presentation and Application layers I can further isolate and protect my network by configuring the connection sessions in isolated and distinct traffic patterns; firewalled then encrypted; ultimately applying the application I need to use, such as NG-911, in a well-protected framework of connectivity.

That is about as simplistic as can be explained for those who don’t understand how to build and protect a network. As you can see there are securing issues at all levels of the applied stack for large-scale telecommunication networks. You should note that “broadband” is just another name for a larger bandwidth service using the same stack methodology – broadband just sounds better. As for Cyber Security (just a fancy word for keeping people out of your stack) we have to insure connectivity and transmission of data is secure at all levels of the network; some of those levels will be controlled locally, some regionally, and some nationally. What FirstNet needs to understand is that it has to define what those roles of responsibility are – not threaten with what they don’t know.

With such complexities why would we think that a centralized-federal-big-government solution would better manage such a network than a small localized State network?

But what the heck do I know I’m...

Just some guy and a blog....